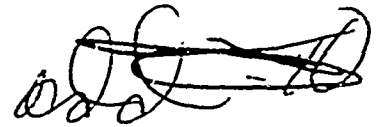


AFCRL-67-0365



RESEARCH TO DEVELOP THE ALGEBRAIC THEORY OF CODES

E. F. Assmus, Jr.  
H. F. Mattson, Jr.  
R. J. Turyn

APPLIED RESEARCH LABORATORY  
SYLVANIA ELECTRONIC SYSTEMS  
A Division of Sylvania Electric Products Inc.  
40 Sylvan Road, Waltham, Massachusetts 02154

Contract No. AF19(628)-5998

Project No. 5628

Task No. 562801

Work Unit No. 56280101

Scientific Report No. 1

June 1967

Contract Monitor  
Vera S. Pless  
Data Sciences Laboratory

Distribution of this document is unlimited. It may be released to the Clearinghouse, Department of Commerce, for sale to the general public.

RECEIVED  
AUG 25 1967  
CFSTI

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES  
OFFICE OF AEROSPACE RESEARCH  
UNITED STATES AIR FORCE  
BEDFORD, MASSACHUSETTS

AD 656783

AFCRL-67-0365

RESEARCH TO DEVELOP THE ALGEBRAIC THEORY OF CODES

E. F. Assmus, Jr.  
H. F. Mattson, Jr.  
R. J. Turyn

APPLIED RESEARCH LABORATORY  
SYLVANIA ELECTRONIC SYSTEMS  
A Division of Sylvania Electric Products Inc.  
40 Sylvan Road, Waltham, Massachusetts 02154

Contract No. AF19(628)-5998

Project No. 5628

Task No. 562801

Work Unit No. 56280101

Scientific Report No. 1

June 1967

Contract Monitor  
Vera S. Pless  
Data Sciences Laboratory

Distribution of this document is unlimited. It may be released to the Clearinghouse, Department of Commerce, for sale to the general public.

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES  
OFFICE OF AEROSPACE RESEARCH  
UNITED STATES AIR FORCE  
BEDFORD, MASSACHUSETTS

## ABSTRACT

A number of new combinatorial designs are found as direct applications of the theory of error-correcting codes. Results on the automorphism groups of Hadamard matrices are presented. A simple proof of the well-known MacWilliams relations, together with a generalization, is given. We have constructed the  $(24,12)$  extended code of Golay over  $GF(2)$  in a particularly simple way. We prove that each of the seven  $6; 2-15-36$  designs  $((v,k,\lambda)$  designs) arising from the difference sets of size 15 in the Abelian groups of order 36 has only the obvious group as automorphism group. Each of these designs gives a Hadamard matrix of order 36.

We determine the covering radius for BCH codes of design distance 2 over  $GF(q)$  for all odd prime powers  $q$ . We give two extensions of the Peterson-Kasami-Lin result on necessary and sufficient conditions for an extension of a cyclic code to be invariant under the affine group. Explicit factorizations of  $x^\ell - 1$  over the appropriate quadratic-number field for  $\ell=7, 11, 13$ , and 23 are given.

## TABLE OF CONTENTS

## NULLIUS. ERRATA FOR OUR 1966 REPORT

- I INTRODUCTION
- II NEW 5-DESIGNS
- III ON THE AUTOMORPHISM GROUPS OF PALEY-HADAMARD MATRICES
- IV ON AUTOMORPHISM GROUPS OF HADAMARD MATRICES
- V GLEASON'S PROOF OF MACWILLIAMS'S RELATIONS
- VI A SIMPLE CONSTRUCTION OF THE BINARY GOLAY CODE
- VII THE (36,15,6) DESIGNS
- VIII THE COVERING RADIUS OF SOME BCH CODES
- IX ON THE PETERSON et al. AFFINE-INVARIANCE THEOREM
- X FACTORIZATION OF  $X^l - 1$  OVER  $Q(\sqrt{\pm l})$ .
- XI A THEOREM OF GLEASON AND PIERCE

## PART NULLIUS

## ERRATA FOR OUR 1966 REPORT

(Final Report, April 28, 1966, AF19(604)-8516)

Page	
III-21	Add to equations (10) [and (11)] the statement "and $n_i \mid m_i$ is even for each $i$ "
III-31	line 15: For " $i \rightarrow i^{-1}$ " read " $i \rightarrow -i^{-1}$ "
III-34	Corollary 1, third line: For "... in $R \mid + \dots$ " read "... in $R, -1 + \dots$ "
IV-3	line-5: For "extensive" read "extension"
IV-7	Reference [7]: Author's last name is Menon

## PART I

## INTRODUCTION

This document contains reports on the scientific work done from May 1, 1966, to April 28, 1967, under the contract named on the cover. The major result is in Part II, "New 5-Designs," where a number of new combinatorial designs are found as direct applications of the theory of error-correcting codes. Results on the automorphism groups of Hadamard matrices, some of which are corollaries of the results of Part II, are presented in Parts III and IV. In Part V we set down A. M. Gleason's simple proof of the well-known MacWilliams relations, together with his generalization of it and our own small point about generalizing this to  $GF(q)$  for  $q$  not prime. In Part VI we have constructed the  $(24,12)$  extended code of Golay over  $GF(2)$  in a particularly simple way. Part VII contains a proof that each of the seven  $6; 2-15-36$  designs  $((\nu, k, \lambda)$  designs) arising from the difference sets of size 15 in the Abelian groups of order 36 has only the obvious group as automorphism group. Each of these designs gives a Hadamard matrix of order 36.

Part VIII determines the covering radius for BCH codes of designs distance 2 over  $GF(q)$  for all odd prime powers  $q$ . Part IX contains two extensions of the Peterson-Kasami-Lin result on necessary and sufficient conditions for an extension of a cyclic code to be invariant under the affine group. Part X contains explicit factorizations of  $x^\ell - 1$  over the appropriate quadratic-number field for  $\ell=7, 11, 13$ , and 23. Part XI is a corrected version of a chapter of our 1965 Report under Contract No. AF19(604)-8516.

Authorship is as follows: E. F. Assmus, Jr. and H. F. Mattson, Jr., Parts II, III, and X; R. J. Turyn, Parts IV, VI, VII, VIII, and XI. Part V as taken from a letter of A. M. Gleason, was slightly edited by us and a short paragraph was added at the end. Part IX is by Mattson and Turyn.

PART II  
NEW 5-DESIGNS  
SECTION 1  
INTRODUCTION

Tactical configurations and Hadamard matrices, studied for many years by combinatorialists, and the newer subject called error-correcting codes, studied for less than twenty years, have some interesting interconnections. The purpose of this report is to establish a number of new results arising therefrom.

Our main result is the construction (via Theorem 4.2) of several new 5-designs on 24 and 48 points and the determination (Section 5) of their automorphism groups as  $\text{PSL}_2(23)$  and  $\text{PSL}_2(47)$ , respectively. A secondary result (Section 5) is that  $\text{PSL}_2(\ell)$  is the automorphism group of certain quadratic-residue codes of length  $\ell+1$  for all primes  $\ell$  having  $(\ell-1)/2$  prime and satisfying  $23 \leq \ell \leq 4,079$ . (For  $\ell=23$  we use [15] and a new 5-design on 24 points; the other cases are an immediate consequence of the Parker and Nikolai search [22].) We have derived elsewhere [7] the consequence that for  $\ell \equiv -1 \pmod{12}$ , the Paley-Hadamard matrix of order  $\ell+1$  has  $\text{PSL}_2(\ell)$  as automorphism group for  $\ell$  as above.

The paper furnishes a setting for the two classical 5-designs and their automorphism groups, the Mathieu groups  $M_{12}$  and  $M_{24}$ , in an infinite class of designs and groups, the designs coming from the vectors of quadratic-residue codes and the groups being the automorphism groups of these codes. The codes are indexed by the prime  $\ell$ , and when  $(\ell-1)/2$  is a prime greater than 5, a result of Ito [15] moreover, implies that the group is either  $\text{PSL}_2(\ell)$  or is 5-fold transitive.

We also establish:

- 1) The existence of two disjoint 5-designs of each of the types found of the smallest "club" size\* (Section 6) and the action of  $\text{PSL}_2(\ell)$  on each of these collections.

---

\*Some of these results were announced in [4].

- 2) The existence of two infinite classes of 3-designs (Theorem 4.1 and Application (3) in Section 4).
- 3) The optimality of "almost all" cyclic codes of a given prime length (Section 2).
- 4) The nonvanishing of all subdeterminants of  $(z^{ij})$ , where  $z$  is a primitive  $\ell$ -th root of 1 and the nonvanishing of all coefficients of all proper divisors of  $x^\ell - 1$  in characteristic 0 (Section 2).

We place in print the Gleason-Prange theorem, that  $\text{PSL}_2(\ell)$  acts on every quadratic-residue code (Section 3).

There seem to be few papers which construct designs from linear codes. Paige [21] found Steiner systems in two codes, although he didn't call his linear spaces "codes." We pursued in [3] the course he had started on, finding for each Mathieu group  $M$  a code with  $M$  as automorphism group, for which the code is a representation-space of smallest possible degree; Paige did this for  $M_{23}$ . We have written other papers on two kinds of Steiner systems [4], [5], [6], all treated by the coding-theory approach presented here. Perhaps the first explicit construction of designs from codes was in Bose's paper [8] on the corrections between error-correcting codes and confounding and fractional replication in the design of experiments. Surprisingly, there do not seem to be any others except a recent Codes - BIBD report [17], although numerous strong implicit connections in the literature likely exist.

In [14] D. R. Hughes considers the problem of constructing  $t$ -designs in relation to the problem of transitively extending groups. His quite different methods yield  $t$ -designs seemingly unrelated to those here, except that the 5-design found there appears here also, since it is intimately related to the Mathieu group  $M_{12}$  (see Section 6).

Acknowledgement. We are indebted to A.M. Gleason, Eugene Prange, and Richard Turyn for many interesting discussions concerning this subject. In particular, Theorem 3.1, on the automorphism groups of quadratic-residue codes, was first proved by Gleason and Prange and our proof is an adaptation of Prange's. Gleason was the first to observe the existence of gaps in the weight-distribution, a fact crucial to the use of Theorem 4.2. We also thank



John Thompson for pointing out to us that the Parker-Nikolai result implied that the automorphism group of the (48,24) code in Section 4 had to be small. Finally, we gratefully acknowledge the help of Nicodemo Ciccia, who wrote the computer programs which suggested the existence of the 8; 5-12-48 design and which helped determine the orbit structure of  $\text{PSL}_2(47)$  on this design.

Definitions of Coding Terms. A code, as defined here in the linear case, is a pair  $(A, S)$ , where  $A$  is a  $k$ -dimensional vector space over a field  $F$ , and  $S$  is a finite set of linear functionals from  $A$  to  $F$  such that they distinguish the points of  $A$ , i.e.,  $x, y \in A$  and  $xf = yf$  for all  $f \in S$  implies  $x = y$ ; this is equivalent to saying that the functionals span the dual space of  $A$ , i.e.,  $\bigcap_{f \in S} \text{Ker } f = 0$ . (We sometimes want to disallow two functional in  $S$  which are scalar multiples of each other and at other times allow the functionals in  $S$  to appear with multiplicities.)

If  $x$  is in  $A$ , the weight of  $x$  is defined to be the number of  $f$  in  $S$  such that  $xf \neq 0$ , and the distance between  $x$  and  $y$  in  $A$  is the weight of  $x - y$ . Distance is translation-invariant.

A concrete realization of the code  $(A, S)$  is the set of all vectors  $(xf_1, \dots, xf_n)$ ,  $x \in A$ , obtained from an ordering  $f_1, \dots, f_n$  of  $S$ . It is a subspace of  $F^n = F \times \dots \times F$  ( $n$  times),  $n$  being the cardinality of  $S$ .  $n$  is called the length of the code. The weight of  $x$  is the number of non-0 coordinates in a concrete realization of the code. This code is called an  $(n, k)$  code over  $F$ . The minimum distance  $d$  from one code-vector to the rest is the same for each starting point, so that the spheres of radius  $\left\lfloor \frac{d-1}{2} \right\rfloor$  about the code-vectors are disjoint. In the rare case that these spheres exhaust  $F^n$ , the code is called perfect.

A cyclic  $(n, k)$  code is one for which some concrete realization is invariant under the permutation of coordinates sending coordinate  $i$  to  $i+1$  (modulo  $n$ ). Such codes can be regarded as ideals in the ring  $F[x]/(x^n - 1)$ , where multiplication by (the residue class of)  $x$  is the cyclic shift. As such, they are principal ideals generated by the divisors of  $x^n - 1$  over  $F$ . Thus, if  $g(x)$  divides  $x^n - 1$ , then all the multiples of  $g(x)$  in  $F[x]$  of degree less than  $n$  constitute a set of representatives of  $(g(x))/(x^n - 1)$ .  $g(x)$  is called the generator polynomial of the code. The concrete code as  $n$ -tuples over  $F$ ,

furthermore, is given recursively by the complementary divisor of  $g(x)$ , by which we mean that if  $g_1(x) \mid g(x) = x^n - 1$ , then the code is the set of all  $(a_0, \dots, a_{n-1})$ ,  $a_i \in F$ , such that

$$\sum_{i=0}^k a_{i+j} b_{k-i} = 0 \quad j = 0, 1, \dots, n-1,$$

where  $g_1(x) = b_0 x^k + \dots + b_k$ . The reader who would like to see more discussion of these points is referred to [23, Chapter 8] or [2, Section IV2].

It is sometimes convenient to construct cyclic codes as follows. Let  $K$  be  $F(z)$  where  $z$  is a primitive  $n$ -th root of 1 over the field  $F$ . Set  $k = [K:F]$ . Let  $f$  be any non-0  $F$ -linear functional on  $K$  as vector space over  $F$ . Then define a set  $S$  of  $n$  coordinate functions  $f_0, \dots, f_{n-1}$  as  $x f_i = (xz^i) f$ ,  $x \in K$ ,  $i = 0, 1, \dots, n-1$ . Then  $(K, S)$  is a cyclic  $(n, k)$  code over  $F$ . This code is immediately seen to be recursive for the reverse of the minimal polynomial of  $z$  (i.e., that of  $z^{-1}$ ) over  $F$ , and it is not hard to prove that the ideal generator polynomial is the complementary divisor. This construction yields only the irreducible cyclic codes, those given recursively by irreducible polynomials; but all cyclic codes are direct sums of irreducible ones.

The orthogonal code to a given code is obtained as the subspace of  $F^n$  orthogonal under the dot product with a given concrete realization of the code. The orthogonal of a cyclic code is cyclic.

The minimum distance of the code  $(A, S)$  over  $F$  is unchanged when we extend the coefficient field  $F$  to an overfield  $L$  by the tensor product [1].

The minimum non-0 weight in an  $(n, k)$  code  $(A, S)$  is the minimum distance and is equal to  $n - m + 1$ , where  $m$  is the least integer such that every subset of  $m$  coordinate functions spans  $S$ . Since  $m$  is necessarily at least  $k$ , it follows that

$$d \leq n - k + 1, \tag{1}$$

where  $d$  is the minimum distance. This bound has been generalized [11,29] to

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d+q^i-1}{q^i} \right\rceil \quad (2)$$

in the case  $F = GF(q)$ .

The square-root bound for cyclic codes is the following: Suppose  $x^n - 1 = (x-1)g_1(x)g_2(x)$  over  $F$ , where  $g_1(x)$  and  $g_2(x)$  both have degree  $(n-1)/2$ . Suppose also that the codes  $A$  and  $B$  having  $g_1(x)$  and  $g_2(x)$ , respectively, as generator polynomials have the same minimum weight  $d$  (as we shall see is often the case). Furthermore, if the minimum weight vectors, as polynomials,

$m(x) = \sum_{i=0}^d a_i x^i$  and  $\sum_{i=0}^d b_i x^i = m_1(x)$ , are not multiples of  $x-1$ , it follows that  $m(x)m_1(x)$  is a scalar multiple of  $x^{n-1} + x^{n-2} + \dots + 1$ . This implies  $d^2 \geq n$ . It is sometimes possible to choose  $f_i \equiv -e_i \pmod{n}$ , and then we get  $d(d-1) \geq n-1$ .

If  $A$  and  $B$  are  $(n,k)$  and  $(n,n-k)$  codes orthogonal to each other over  $GF(q)$ , and  $A_i, B_i$  denote the number of vectors of  $A, B$  of weight  $i$ , then MacWilliams has proved [20] that

$$\sum_{i=0}^{n-\nu} A_i \binom{n-i}{\nu} = q^{k-\nu} \sum_{i=0}^{\nu} B_i \binom{n-i}{n-\nu}, \quad \nu = 0, 1, \dots, n. \quad (3)$$

These MacWilliams identities are basic to our main result, Theorem 4.2.

**BLANK PAGE**

## PART II

## SECTION 2

## OPTIMAL CODES

Motivated by the inequality (1), we call an  $(n,k)$  code optimal if  $d = n-k+1$ . The  $(n,1)$  code  $\{(\alpha, \alpha, \dots, \alpha); \alpha \in GF(q)\}$  is optimal, and the main result of this section is that "almost all" cyclic codes of prime length are optimal.

Let  $\ell$  be prime and consider all the cyclic codes of length  $\ell$  over  $GF(\ell) = F$ . Since  $x^\ell - 1 = (x-1)^\ell$  over  $F$ , these codes, considered as ideals in  $F[x]/(x^\ell - 1)$ , are the ideals  $A_i = (x-1)^i$  for  $i = 0, 1, \dots, \ell$ . Thus they satisfy

$$(1) = A_0 \supsetneq A_1 \supsetneq \dots \supsetneq A_\ell = (0) .$$

The dimension of  $A_i$  is  $\ell-i$ . The minimum weight in  $A_i$  is easy to determine directly: If  $f(x)$  is a minimum-weight polynomial in  $A_i$ ,  $i=1, \dots, \ell-1$ , cycled so that the constant term is not 0, then  $f'(x)$  is a vector in  $A_{i-1}$  with weight 1 less than that of  $f(x)$ . Therefore, if  $d_i$  denotes the minimum weight in  $A_i$ , we have

$$1 = d_0 < d_1 < \dots < d_{\ell-1} = \ell$$

since we have  $d_0 = 1$  and  $d_{\ell-1} = \ell$  by inspection. Therefore  $d_i = i+1$  for  $i = 0, 1, \dots, \ell-1$ . We have proved

LEMMA. The cyclic  $(\ell,k)$  codes of prime length  $\ell$  over  $GF(\ell)$  are all optimal.

THEOREM 2.1. Let  $\ell$  be prime and let  $z$  be a primitive  $\ell$ -th root of 1 over the rational field  $Q$ . Let  $E$  be any subfield of  $K = Q(z)$  and let  $A$  be a cyclic  $(\ell,k)$  code over  $E$ . Then the minimum weight of  $A$  is  $\ell-k+1$ .

Proof. The module consisting of all code-vectors of  $A$  with coordinates in  $\mathcal{O}$ , the integers of  $E$ , has the same minimum weight that  $A$  has. The ideal  $\mathcal{O}\ell$  is a power of a principal prime ideal, of  $\mathcal{O}$ , of degree 1. If we reduce by the residue-class map of this prime ideal we obtain a cyclic  $(\ell, k)$  code over  $GF(\ell)$ , which, by our Lemma, has minimum weight  $\ell - k + 1$ . If  $d$  denotes the minimum weight of  $A$ , then  $d \leq \ell - k + 1$ , in general; and we have just proved  $d \geq \ell - k + 1$ , since there are minimum weight code-vectors in the module not all coordinates of which are in the principal prime ideal.

COROLLARY. Any proper divisor of  $x^\ell - 1$  over  $Q(z)$  has all coefficients non-0.

REMARKS. 1. Enlarging the base field  $E$  preserves the optimality in view of the result in Section 1 on tensor products.

2. This theorem furnishes a simple indirect proof of the following: Let  $r = [K:E]$ . Then every set of  $r$  distinct powers of  $z$  is linearly independent over  $E$ . We can even conclude from the present theorem that every subdeterminant of the  $\ell \times \ell$  determinant  $(z^{ij})$  is nonvanishing. We do this by first considering an arbitrary  $(\ell, k)$  cyclic code over  $K$  given recursively by  $(x - z^{e_1}) \dots (x - z^{e_k})$ ,  $0 \leq e_i < \ell$ , the  $e_i$ 's distinct modulo  $\ell$ . This code consists of the space  $K \times \dots \times K$  ( $k$  times) and the coordinate functions  $f_j$  defined by

$$(c_1, \dots, c_k) f_j = c_1 z^{e_1 j} + \dots + c_k z^{e_k j}$$

$c_1, \dots, c_k \in K$ ,  $j = 0, 1, \dots, \ell - 1$ . That is, it is the direct sum of the codes

$(c_i, c_i z^{e_i}, c_i z^{2e_i}, \dots, c_i z^{(\ell-1)e_i})$  for  $i = 1, \dots, k$ . By Theorem 2.1 and the preceding remark, this code has optimal minimum weight. Therefore every set of  $k$  coordinate functions is linearly independent over  $K$ . But if for some  $k$  choices of  $j$ , say  $t_1, \dots, t_k$ , the determinant  $|z^{e_i t_j}|$  vanished, then it would follow that  $f_{t_1}, \dots, f_{t_k}$  were linearly dependent over  $K$ .

THEOREM 2.2. Let  $\ell$  be a prime. Then for all but a finite number of primes  $p$ , each cyclic code of length  $\ell$  over  $GF(p^1)$  is optimal (for all  $i$ ).

Proof. A cyclic  $(\ell, k)$  code over  $GF(q)$  is optimal if and only if every  $k \times k$  determinant in  $(\zeta^{je_i})$ , for  $i=1, \dots, k$ , and  $j=0, \dots, \ell-1$ , is nonvanishing, where the code is defined recursively by  $(x-\zeta^{e_1}) \dots (x-\zeta^{e_k})$ . Such determinants are the images under residue-class maps of the nonvanishing global determinants in  $(z^{je_i})$ . These determinants are non-0 integers in  $K$  and are, therefore, dividible by only a finite number of primes. QED.

We have proved the following result for the linear case [1], and it has also been proved more generally, in [27] and implicitly in [26], which note a connection with latin squares. We omit the proof here.

THEOREM 2.3. If an  $(n, k)$  code over  $GF(q)$  is optimal, then  $q-1 \geq \min\{k, n-k\}$ . Furthermore, if  $1 < k < n-1$  (i.e., if this minimum is at least 2), then  $q-1 \geq \max\{k, n-k\}$ .

We note that the conclusion of this Theorem is not sufficient to give an optimal code. For example, one could extend the coefficient-field of any non-optimal code.

**BLANK PAGE**



## PART II

## SECTION 3

## ON AUTOMORPHISM GROUPS OF CODES

In this section we prove a basic result due to Gleason and Prange on the automorphism group of an extended quadratic-residue code, to be defined. We will then find some corollaries on weights in codes.

An invariance of a code  $(A, S)$  is a linear transformation  $\sigma$  of  $A$  onto  $A$  such that for each  $f$  in  $S$ ,  $\sigma f = \alpha g$  for some scalar  $\alpha$  (depending on  $f$ ) and some  $g$  in  $S$ . In terms of the concrete realization of the code,  $\sigma$  is a monomial matrix which preserves the code-space. An invariance preserves the weight of each code-vector. For example, the cyclic shift is an invariance of a cyclic code.

The automorphism group of the code is the group of all invariances modulo scalar multiplications. In this report we are mainly concerned with the permutation aspects of the automorphism group, so we remark that the mapping which sends each invariance to its underlying permutation is a homomorphism of the invariance group which sends the scalar multiplications to the identity permutation; therefore, we shall often speak of this or that permutation group as being "contained in" the automorphism group of the code.

We now prove that the projective unimodular group  $PSL_2(\ell)$  is "contained in" the automorphism group of the extended quadratic-residue codes, defined below.

Let  $\ell$  be an odd prime and let  $z$  be a primitive  $\ell$ -th root of unity over the field  $Q$  of rational numbers. Let  $K = Q(z)$  be the cyclotomic field of all  $\ell$ -th roots of 1 over  $Q$ . Then  $K/Q$  is a cyclic extension of degree  $\ell-1$ , and  $K$  contains a unique subfield  $L$  of degree 2 over  $Q$ .  $L$  is, in fact, generated by  $\eta = \sum z^r$ , the sum being taken over the quadratic residues  $r$  modulo  $\ell$ , since  $\eta = T_{K/L}(z)$ . The irreducible polynomial for  $\eta$  over  $Q$  is  $x^2 + x + (1 \pm \ell)/4$ , where the sign is chosen to make  $(1 \pm \ell)/4$  an integer. Thus  $L = Q(\sqrt{\pm \ell})$ , and the sign is that in  $\ell \equiv \pm 1 \pmod{4}$ . The polynomial  $x^{\ell-1} + \dots + 1$ ,

which is irreducible over  $Q$ , splits into  $g_1(x) g_2(x)$ , irreducibles of degree  $(\ell-1)/2$  over  $L$ . There are cyclic  $(\ell, (\ell+1)/2)$  codes over  $L$  denoted as follows:

$A$ , recursive for  $g_1(x)$ , generated as ideal by  $(x-1) g_2(x)$ .

$A^+$ , recursive for  $(x-1) g_1(x)$ , generated as ideal by  $g_2(x)$ ;  $A \perp A^+$ .

$B$  and  $B^+$  are defined by interchanging  $g_1(x)$  and  $g_2(x)$  above. These are called global quadratic-residue codes, since

$$g_1(x) = \prod_{r \in R} (x-z^r), \quad g_2(x) = \prod_{s \in R'} (x-z^s)$$

where  $R$  and  $R'$  are, respectively, the quadratic residues and nonresidues modulo  $\ell$ .

$A$  and  $B$  have the same weight distributions (so do  $A^+$  and  $B^+$ ), because the permutation of coordinates sending  $i$  to  $si$  for each  $i = 0, 1, \dots, \ell-1$  for any fixed quadratic nonresidue  $s$  modulo  $\ell$  interchanges the two codes.

As Gleason and Prange [9], [25] observed in the finite case, these codes can be embedded in spaces of  $\ell+1$  dimensions in a nice way which allows the projective unimodular group to act. We now carry over Prange's construction to the present global situation.

We first embed the codes. The coordinate functions for  $A^+$  are the  $f_j$ :  $L \times K \rightarrow L$  defined by

$$(c_0, c) f_i = c_0 + T_{K/L}(cz^i) \quad c_0 \in L, \quad c \in K,$$

$i = 0, 1, \dots, \ell-1$ . Similarly for  $B$ , with  $z$  replaced by  $z^s$  for some fixed  $s \in R'$ .  $A$  is the subcode of  $A^+$  given by restricting the  $f_i$  to  $0 \times K$ , i.e., by setting  $c_0 = 0$ .  $A$  will embed as a subcode of  $A^+$  so we define the embedding for  $A^+$ . We will introduce a new coordinate function

$$f_\infty = \gamma \sum_{i=0}^{\ell-1} f_i$$

for some  $\gamma \in L$  to be chosen so that the new code, called  $A_\infty$ , will be orthogonal to itself or to the corresponding new code  $B_\infty$  for  $B^\dagger$ .  $A_\infty$  and  $B_\infty$  are called extended quadratic-residue codes.

Observe that  $(c_0, c) f_\infty = \gamma \ell c_0$ ; letting  $f'_1$  and  $f'_\infty$  be the coordinate functions for  $B_\infty$  with  $f'_\infty = -\gamma \sum f'_i$ , we get  $(c_0, c) f'_\infty = -\gamma \ell c_0$ .

$A$  is the subcode of  $A_\infty$  with "infinite" coordinate equal to 0.

Orthogonality depends on the congruence of  $\ell$  modulo 4. The results are summarized here before embedding:

$$\ell \equiv -1 \pmod{4}$$

$$A^\perp = A^+$$

$$B^\perp = B^+$$

$$\ell \equiv +1 \pmod{4}$$

$$A^\perp = B^+$$

$$B^\perp = A^+$$

Thus, after embedding, we have

$$A_\infty^\perp = \begin{cases} A_\infty & \ell \equiv -1 \pmod{4} \\ B_\infty & \ell \equiv +1 \pmod{4} \end{cases}$$

provided only that  $\langle 1, 0 \rangle = (1, 1, \dots, 1; \ell\gamma)$  is orthogonal to itself or to the corresponding vector in  $B_\infty$ , which is to say

$$\begin{aligned} 1 + \ell\gamma^2 &= 0 & \ell &\equiv -1 \pmod{4} \\ 1 - \ell\gamma^2 &= 0 & \ell &\equiv +1 \pmod{4} \end{aligned} \tag{1}$$

Thus  $\gamma$  is determined up to sign as  $1/\sqrt{\pm \ell}$ , which is in  $L$  as it should be.

The invariance group of  $A_\infty$  obviously contains the cyclic shift  $\tau$  on the "finite"  $f_i$  ( $\tau$  fixes  $f_\infty$ ); similarly for  $B_\infty$ . It also contains the Galois automorphisms  $\rho_r$ , which send  $f_i$  to  $f_{ri}$ ,  $i = 0, \dots, \ell-1$ ;  $r \in R$ ; these also fix  $f_\infty$ .

We now prove that a certain interchange of  $f_0$  and  $f_\infty$  is an invariance  $\sigma$  of  $A_\infty$ ; also, the permutation parts of  $\sigma$ ,  $\tau^1$ , and  $\rho_r$  generate the (one-dimensional) projective unimodular group over  $GF(\ell)$ . The same will hold for  $B_\infty$ . (The projective unimodular group,  $PSL_2(\ell)$ , is the group of all  $2 \times 2$  matrices over  $GF(\ell)$  with determinant 1 modulo the center  $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ . Elements of this group can be factored as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1/c \end{pmatrix}$$

provided  $c \neq 0$ .)

We define  $\sigma$  as follows: As permutation on the coordinate functions  $\sigma$  sends  $f_i$  to  $f_{-1/i}$  (subscripts modulo  $\ell$ ), interchanging  $f_0$  and  $f_\infty$ . Signs are introduced via the Legendre symbol; thus  $\sigma f_i = \epsilon_i f_{-1/i}$ , where  $\epsilon_i = (i/\ell)$   $i=1, \dots, \ell-1$ . We shall choose  $\epsilon_0$  and  $\epsilon_\infty$  later, as  $\pm 1$ . Thus

$$(a_0, \dots, a_{\ell-1}; a_\infty) \sigma = (\epsilon_0 a_\infty, \dots, \epsilon_i a_{-1/i}, \dots, \epsilon_\infty a_0)$$

We must prove that with proper choice of  $\epsilon_0$  and  $\epsilon_\infty$ ,  $\sigma$  maps  $A_\infty$  onto itself and also that this  $\sigma$  maps  $B_\infty$  onto itself.

Case 1:  $\ell \equiv -1 \pmod{4}$ . Since  $A_\infty = L < 1, 0 > \oplus A$ , it suffices to show  $< 1, 0 > \sigma \in A_\infty$  and  $A\sigma \subset A_\infty$ . Thus  $< 1, 0 > \sigma = (1, 1, \dots, 1; \ell\gamma) \sigma = (\epsilon_0 \ell\gamma, \dots, \epsilon_i, \dots; \epsilon_\infty)$ ; and therefore

$$< 1, 0 > \sigma^2 = (\epsilon_0 \epsilon_\infty, -1, \dots, -1; \epsilon_0 \epsilon_\infty \gamma \ell)$$

since  $\epsilon_i \epsilon_{-1/i} = (-1/\ell) = -1$ . This vector obviously cannot be in  $A_\infty$  unless  $\epsilon_0 \epsilon_\infty = -1$ . Thus we choose

$$\epsilon_\infty = -\epsilon_0 = -\epsilon \tag{2}$$

Now  $\langle 1, 0 \rangle \sigma$  is in  $A_\infty$  if and only if it annihilates  $A_\infty$  under the usual dot-product. This means that we must find  $\epsilon\gamma\ell + \sum_{i=1}^{\ell-1} \epsilon_i - \epsilon\gamma\ell = 0$  as is indeed the case; and also we need  $\langle 1, 0 \rangle \sigma \perp \langle 0, c \rangle$  for all  $c \in K$ . That is, we must also have

$$(\epsilon\gamma, \dots, \epsilon_i, \dots; -\epsilon) \cdot (T(c), \dots, T(cz^i), \dots; 0) = 0,$$

or

$$\epsilon\gamma T(c) + \sum_{r \in R} T(cz^r) - \sum_{s \in R'} T(cz^s) = \epsilon\gamma T(c) + (\eta - \eta')T(c) = 0,$$

where  $\eta = \sum z^r (r \in R)$  and  $\eta' = \sum z^s (s \in R')$ , and we make use of the L-linearity of  $T$ , which denotes the trace from  $K$  to  $L$  here. Thus  $\sigma$  maps  $A_\infty$  onto  $A_\infty$  if and only if  $\epsilon$  and  $\gamma$  are chosen so that

$$\epsilon\gamma + \eta - \eta' = 0 \quad (3)$$

Now from (1),  $(\gamma\ell)^2 = -\ell$ , so  $\ell\gamma = \pm\sqrt{-\ell}$ , and  $\eta - \eta'$  is also either  $\sqrt{-\ell}$  or  $-\sqrt{-\ell}$ , so  $\epsilon$  must be taken as  $\pm 1$ . The choice depends on the choice of notation for  $g_1(x)$  and  $g_2(x)$ . We chose  $z$  to be a root of  $g_1(x)$ ; thus  $\eta$  is the negative of the coefficient of  $x^{(\ell-3)/2}$  in  $g_1(x)$ . Thus the choice of notation determines the sign of  $\epsilon\gamma$ , and we are free to choose  $\epsilon = 1$  or  $\epsilon = -1$ .

We now show that  $\langle 0, c \rangle \sigma \perp A_\infty$  for all  $c \in K$ . Now  $\langle 0, c \rangle \sigma = (0, \dots, \epsilon_i T(cz^{-1/i}), \dots; -\epsilon T(c)) = (a_0, a_1, \dots; a_\infty)$  is in  $A_\infty$  if and only if the polynomial  $\sum a_i x^i$  is a multiple of  $g_1(x)$ , since  $\gamma \sum_{i=0}^{\ell-1} a_i = \gamma(\eta' - \eta)T(c) = \epsilon\gamma^2 T(c) = -\epsilon T(c)$ , from (2) and (1). Now  $g_1(x)$  is irreducible and has  $z$  as a root; therefore  $\langle 0, c \rangle \sigma \in A_\infty$  if and only if the quantity  $D(c) = 0$  for all  $c \in K$ , where  $D(c)$  is defined as

$$D(c) = \sum_{i=1}^{\ell-1} \epsilon_i T(cz^{-1/i}) z^i$$

If  $\tau$  is any automorphism of  $K/Q$ , such that  $z^\tau = z^t$ , then

$$D(c)^\tau = \epsilon_t D(c^{\tau^{-1}})$$

as one can easily verify using  $T(c)^\tau = T(c^\tau)$ . Since  $D$  is linear and  $z, z^2, \dots$  span  $K/L$ , it suffices to prove  $D(z) = 0$ . Now,

$$\begin{aligned} D(z) &= \sum_{i=1}^{\ell-1} \epsilon_i T(z^{1-1/i}) z^i \\ &= \sum_{i=1}^{\ell-1} \epsilon_i \sum_{r \in R} z^{r(1-1/i)} z^i \\ &= \sum_{i,r} \epsilon_i z^{r-r/i + i} \end{aligned}$$

This is a polynomial in  $z$  of degree at most  $\ell-1$  with integral coefficients. For each  $k = 0, 1, \dots, \ell-1$  we find the coefficient of  $z^k$  as  $\sum_{r,i} \epsilon_i$  where  $i$

runs over the solutions of  $r-r/i + i \equiv k \pmod{\ell}$ . These  $i$  are the same as those for which  $i^2 + (r-k)i - r \equiv 0 \pmod{\ell}$ . The polynomial  $x^2 + (r-k)x - r$  never has double roots in  $GF(\ell)$  since the constant term is in  $R'$ . Thus for each value of  $k$  and  $r$  there are two distinct roots  $i$  and  $i'$ ; one is in  $R$ , the other in  $R'$ . Thus the polynomial in  $z$  is identically 0. This completes the proof that  $\sigma$  maps  $A_\infty$  onto itself.

PROPOSITION 3.1. If we embed  $A$  with  $\gamma$  and  $B$  with  $-\gamma$ , then there is a choice of  $\epsilon = \pm 1$ , given in (3), such that  $\sigma$  maps each of  $A_\infty$  and  $B_\infty$  onto itself.

CAUTION. We have defined  $\sigma$  monomially on  $L^{\ell+1}$ .  $L \times K$  is embed in  $L^{\ell+1}$  in distinct ways as  $A_\infty$  and  $B_\infty$ . The linear transformations of  $L \times K$  induced by  $\sigma$  are distinct.

Case 2.  $\ell \equiv +1 \pmod{4}$ . We must use  $\gamma$  to embed A and  $-\gamma$  to embed B in order to make  $A_\infty^1 = B_\infty$  in this case, where  $\ell\gamma^2 = 1$ . We define  $\sigma$  as before and find that  $\langle 1, 0 \rangle \sigma^2 \in A_\infty$  if and only if  $\epsilon_0 \epsilon_\infty = 1$ . We take

$$\epsilon = \epsilon_0 = \epsilon_\infty = \pm 1 \quad (4)$$

Now  $\langle 1, 0 \rangle \sigma$  is in  $A_\infty$  if  $\langle 1, 0 \rangle \sigma$  annihilates B and the vector  $\langle 1, 0 \rangle$ ; the former happens if and only if, as before,

$$\epsilon\gamma\ell - (\eta - \eta') = 0 \quad (5)$$

Proceeding as in Case 1 we can verify that  $\gamma$  and  $\epsilon$  are related by (5).

If we ask whether this same  $\sigma$  maps  $B_\infty$  onto itself, then the part relating to  $\langle 1, 0 \rangle$  goes through, since in (5) we replace  $\gamma$  by  $-\gamma$  and interchange  $\eta$  and  $\eta'$ . The rest goes through too; the part involving  $D(c)$  is formally the same. We have proved

**PROPOSITION 3.2.** If  $\ell \equiv +1 \pmod{4}$  and we use  $\gamma$  to embed A,  $-\gamma$  to embed B, then  $A_\infty$  and  $B_\infty$  are orthogonal to each other and  $\sigma$  maps each onto itself.  $\epsilon$  and  $\gamma$  are chosen by (4) and (5).

We are equally interested in the finite codes obtained from  $A_\infty$  and  $B_\infty$  by mapping the integral submodules of these via the residue-class maps of primes in L lying over the rational prime p. These codes we denote by  $A_p$  (or  $B_p$ ); they are finite, extended quadratic residue codes of type  $(\ell+1, (\ell+1)/2)$  over  $\text{GF}(q)$ , where  $q = p$  or  $p^2$  depending on whether p is or is not a quadratic residue modulo  $\ell$ .

In the rest of the report we often refer for short to "the"  $(\ell+1, \frac{\ell+1}{2})$  code over  $\text{GF}(p)$  (or  $p^2$ ), by which we mean the code  $A_p$  or  $B_p$  just defined; because of their equivalence under a monomial transformation, it usually does not matter which one we consider.

With Propositions 3.1 and 3.2 we have essentially proved

**THEOREM 3.1.** The automorphism groups of the two extended quadratic-residue codes  $A_\infty$  and  $B_\infty$  each contains a subgroup of which the permutation part is precisely  $\text{PSL}_2(\ell)$ . The same statement holds for the finite codes  $A_p$  and  $B_p$ .

Proof. We have proved this in the global case. Formally the same proof works in the finite case; or one can project the group generated by the invariances  $\rho_\tau$ ,  $\tau$ , and  $\sigma$  defined globally above (the permutations of which generate  $\text{PSL}_2(\ell)$  by the residue-class map, noting that all scalars involved in the definitions of these invariances are  $\pm 1$ ).

**COROLLARY.** The minimum distance in  $A^+$  is 1 less than that in  $A$ ; the same for the corresponding finite codes over any  $\text{GF}(q)$  for which  $(q/\ell) = +1$ . In particular, the square-root bound holds for these codes.

A. M. Gleason has also proved Theorem 3.1 by means of induced representations, and M. Hall, Jr., has proved essentially this result, but stated for Paley-Hadamard matrices [12, Theorem 2.1] for the case  $\ell \equiv -1 \pmod{4}$ .

When  $\ell \equiv -1 \pmod{4}$  we can use the self-orthogonality of  $A_\infty$  and  $B_\infty$  to get some results on the weight-distributions of these codes over  $\text{GF}(2)$  and  $\text{GF}(3)$ .

**THEOREM 3.2** Let  $\ell \equiv -1 \pmod{4}$ . If  $(2/\ell) = +1$ , then  $A_2$  and  $B_2$  have all weights divisible by 4. If  $(3/\ell) = +1$ , then  $A_3$  and  $B_3$  have all weights divisible by 3.

Proof. We first remark that the set of cyclic shifts of any vector  $(c_0, c)$  in  $A^+$  spans the entire code  $A^+$  if  $c_0 c \neq 0$ . This is true because  $A^+$  is the direct sum of the irreducible cyclic code  $A$  and the "all-1" code  $\{\alpha(1, \dots, 1); \alpha \in L\}$ . This result therefore holds for  $A_\infty$  and hence for the codes  $A_p$ .

When  $\ell = 8N-1$ , 2 is in  $R$ , the set of quadratic-residues modulo  $\ell$ , and the weight- $4N$  vector  $a = (a_i)$  with  $a_i = 1$  for  $i \in R$  and  $i = \infty$ , and with  $a_i = 0$  otherwise, is in  $A_2$ . Since  $A_2$  is self-orthogonal, any two code-vectors must have an even number of places with 1's in common; this implies that any sum of shifts of  $a$  has weight divisible by 4. (A.M. Gleason was the first to observe this.)



In the GF(3) case the matter is very simple. Each vector  $(a_0, \dots, a_{\ell-1}; a_\infty)$  is in particular orthogonal to itself, so

$$a_\infty^2 + \sum_{i=0}^{\ell-1} a_i^2 = 0$$

But the non-0 a's are  $\pm 1$ , so their number must be a multiple of 3.

COROLLARY. The extended (24,12) quadratic-residue code over GF(3) has minimum weight 9.

Proof. It is greater than 6 by the square-root bound and it is less than 12 by (2) of Section 1.

It is also true that the extended quadratic-residue codes over GF(4) for  $\ell = 8N+5$  have all weights even. Moreover, 2, 3, and 4 are the only values of  $q$  for which extended quadratic-residue codes can have "regular" gaps in their weight distributions [30]; for  $q = 2$  one might have all weights even or multiples of 4, for  $q = 3$  all weights may be multiples of 3, and for  $q = 4$  all weights may be even; but no larger divisors are possible.

The special cases of the above for  $\ell = 23$ ,  $q = 2$  and  $\ell = 11$ ,  $q = 3$  are closely related to the Mathieu groups. For proofs that in the first case, the automorphism group is  $M_{24}$ , and in the second case,  $M_{12}$ , the reader should consult [3].

**BLANK PAGE**

## PART II

## SECTION 4

## COMBINATORIAL DESIGNS ASSOCIATED WITH CERTAIN CYCLIC CODES

A tactical configuration of type  $\lambda; t-d-n$ , or t-design, is a collection  $\mathcal{D}$  of  $d$ -subsets\* of a given  $n$ -set  $S$  such that every  $t$ -subset of  $S$  is contained in precisely  $\lambda$  members of  $\mathcal{D}$ . Here  $\lambda$  is a positive integer; and  $0 \leq t \leq d \leq n$ , where if any equality obtains we call the design trivial. Balanced incomplete block designs are 2-designs with restrictions on  $d$  and  $n$ ; where  $\lambda = 1$  the  $t$ -design is called a Steiner system; Steiner triple systems are 1; 2-3- $n$  tactical configurations; and projective spaces contain several 2-designs, for example. Also,  $(v, k, \lambda)$  configurations are special cases of  $\lambda; 2-k-v$  designs.

The automorphism group of a  $t$ -design is the group of all permutations of  $S$  which map each member of  $\mathcal{D}$  onto a member of  $\mathcal{D}$ .

For convenience we often call the members of  $\mathcal{D}$  clubs or d-clubs. A  $t$ -design is automatically a  $t'$ -design for  $t' < t$ . Also, the clubs of a given  $\lambda; t-d-n$  design containing a fixed point  $P$  of  $S$  form a  $(t-1)$ -design on  $S-P$  when  $P$  is removed from these clubs. The new parameters are  $\lambda; (t-1) - (d-1) - (n-1)$ .

No one has discovered nontrivial  $t$ -designs for  $t$  larger than 5. Two essentially unique 5-designs, the Steiner systems associated with the Mathieu group  $M_{12}$  and  $M_{24}$ , have been known for many years, however; and recently [3] [14] two disjoint Steiner systems of these types were constructed, meaning that 2; 5-6-12 and 2; 5-8-24 designs exist (see also Section 6). Aside from these and such designs obtainable as certain orbits of  $M_{12}$  and  $M_{24}$  (see below), which have been at least implicitly known for a long time, no other nontrivial 5-designs were known until recently. The main purpose of this section is to derive all of the above designs, except perhaps for some of the "orbit-designs" just mentioned, and several new 5-designs which are not "orbit-designs," by means of coding theory. Another purpose is to exhibit two infinite classes of 3-designs (Theorem 4.1 and Application (3)).

---

\*An  $x$ -set is a set of cardinality  $x$ .

Such designs can arise from codes as follows. From a given code consider the set of all vectors of a certain weight  $w$ . For each such vector consider the set  $D$  of all coordinate places at which the vector is not 0.  $D$  is thus said to hold a code-vector of weight  $w$ . For certain codes and certain values of  $w$ , the collection of all such sets  $D$  forms a  $t$ -design for  $t$  as high as 5. For example, we showed this for  $t = 5$  for the minimum-weight vectors of the finite extended quadratic-residue codes of type  $(24,12)$  over  $GF(2)$  and  $(12,6)$  over  $GF(3)$  by direct special methods in [3]. In different terms this was also done for the  $(23,12)$  and  $(11,6)$  codes for  $t = 4$  by Paige [21]. We shall derive these and all the other cases as applications of Theorem 4.2 below.

We begin with the following simple remark.

**PROPOSITION.** A code is optimal if and only if the minimal-weight vectors yield a trivial design.

Proof. Suppose it is an  $(n,k)$  code of minimum weight  $d$ , such that every  $d$ -subset of coordinate places holds a code-vector. We wish to prove that  $d = n-k+1$ . Consider the subcode  $C$  spanned by the minimum-weight vectors: the orthogonal code to  $C$  has every subset of  $d$  coordinate-functions linearly dependent, but no subset of size  $d-1$  with this property; it therefore has dimension  $d-1$ , so that  $C$  has dimension  $n - (d-1) \leq k$ . The reverse inequality holds in general, by (1) of Section 2.

Conversely, if  $d = n-k+1$ , then every  $k$  coordinate functions are linearly independent. Given a  $d$ -subset of coordinate functions, we consider the  $n-d = k-1$  functions of the complementary subset. The intersection of the kernels of these is non-0; a non-0 vector in it must have weight  $d$ . QED.

The following result is an immediate consequence of Theorem 3.1 and the fact that the  $PSL_2(\ell)$  is 2-fold transitive, in general, and 3-set transitive when  $\ell = 4N-1$ . Also,  $PGL_2(\ell)$  is 3-fold transitive and acts on  $A_\infty \cup B_\infty$ .

**THEOREM 4.1.** The finite extended quadratic-residue codes of length  $\ell+1$  yield 2-designs for all  $\ell$  and 3-designs when  $\ell \equiv -1 \pmod{4}$ , from every weight-class of code-vectors. Also, in all cases the union of  $A_p$  and  $B_p$  yields 3-designs from each weight class.

Remark. In view of the proposition above and Theorem 2.3, we have that the minimum weight vectors in  $A_p$  always yield a nontrivial design (on which  $PSL_2(\ell)$  acts) whenever  $q-1 < \frac{\ell+1}{2}$ . (Recall that  $q = p$  or  $p^2$  depending on whether  $p$  is a quadratic residue modulo  $\ell$  or not.) In particular then,  $A_2$  yields a nontrivial design whenever  $\ell > 5$  and, of course,  $d \leq \frac{\ell+1}{2}$ ,  $d(d-1) \geq \ell-1$ . The determination of  $d$  seems to be, in general, a difficult problem.

Let  $A$  and  $B$  be linear orthogonal  $(n, k)$  and  $(n, n-k)$  codes over  $GF(q)$  with minimum weights  $d$  and  $e$ . Let  $t$  be an integer less than  $d$ . Let  $v_0$  be the largest integer satisfying  $v_0 - \left\lfloor \frac{v_0 + (q-2)}{q-1} \right\rfloor < d$ , and  $w_0$  the largest integer satisfying  $w_0 - \left\lfloor \frac{w_0 + (q-2)}{q-1} \right\rfloor < e$ , where, if  $q = 2$ , we take  $v_0 = w_0 = n$ . (Such a restriction ensures that two vectors of  $A$  with weight at most  $v_0$  having their non-0 coordinates in the same places must be scalar multiples of each other.)

**THEOREM 4.2.** Suppose that the number of non-0 weights of  $B$  which are less than or equal to  $n-t$  is itself less than or equal to  $d-t$ . Then, for each weight  $v$  with  $d \leq v \leq v_0$ , the vectors of weight  $v$  in  $A$  yield a  $t$ -design, and for each weight  $w$  with  $e \leq w \leq \text{Min}\{n-t, w_0\}$ , the vectors of weight  $w$  in  $B$  yield a  $t$ -design.

Before proving the above result we remark that for  $B$  we will in fact show that for each weight  $w$ , with  $e \leq w \leq \text{Min}\{n-t, w_0\}$ , the vectors of weight  $w$  yield blocks the complements of which form a  $t$ -design. We will need the following combinatorial

**LEMMA.** Suppose  $(S, \mathcal{D})$  is a  $t$ -design. Then, if  $T$  and  $T'$  are two  $t$ -subsets of  $S$ , and  $k$  an integer satisfying  $0 \leq k \leq t$ , we have that

$$\left| \left\{ D \in \mathcal{D}; |D \cap T| = k \right\} \right| = \left| \left\{ D \in \mathcal{D}; |D \cap T'| = k \right\} \right|.$$

That is, the number of subsets in  $\mathcal{D}$  striking a given  $t$ -subset precisely  $K$  times is independent of the chosen  $t$ -subset.

Proof. For  $k=t$  the assertion is simply the condition that  $(S, \mathcal{D})$  is a  $t$ -design. Now we use induction downwards observing that for  $K \subseteq T$ ,  $|K| = k$ , we have that

$$\left| \{D \in \mathcal{D}; K \subseteq D\} \right| = \frac{\lambda \binom{n-k}{t-k}}{\binom{d-k}{t-k}} = \lambda_k$$

where  $(S, \mathcal{D})$  has parameters  $\lambda; t-d-n$ , and hence that

$$\left| \{(K, D); K \subseteq D, K \subseteq T, |K| = k\} \right| = \binom{t}{k} \lambda_k.$$

Then an inclusion-exclusion argument yields the result.

COROLLARY. The complement of a  $t$ -design is a  $t$ -design.

(Here, if  $(S, \mathcal{D})$  is a  $t$ -design, then its complement is  $(S, \{S-D; D \in \mathcal{D}\})$ . Of course, if  $n-d < t$  it is trivially so.) Complementary  $t$ -designs have parameters  $\lambda; t-d-n$  and  $\lambda'; t-(n-d)-n$ , where  $\lambda' = \lambda \binom{n-d}{t} \div \binom{d}{t}$ .

Proof of the Theorem. If  $T$  is a coordinate set with  $|T| = t$  we denote by  $A^T$  the code of length  $n-t$  obtained by neglecting the coordinates in  $T$ . We denote by  $B^{0 \vee T}$  the code of length  $n-t$  obtained from the vectors in  $B$  which have 0's at the coordinates in  $T$  by neglecting those coordinates. Clearly,  $A^T \perp B^{0 \vee T}$ . Since every  $n-d+1$  coordinate functionals of  $A$  span and  $t < d$ ,  $A^T$  is an  $(n-t, k)$  code. Since the vectors of  $A$  are the relations on the functionals of  $B$  and  $t < d$ , the functionals corresponding to the coordinates in  $T$  are linearly independent and  $B^{0 \vee T}$  is an  $(n-t, n-k-t)$  code. Thus,  $A^T$  and  $B^{0 \vee T}$  are orthogonal. Let  $0 < v_1 < v_2 < \dots < v_{d-t} \leq n-t$  be the possible non-0 weights less than or equal to  $n-t$  appearing in  $B$ . Then the only non-0 weights appearing in  $B^{0 \vee T}$  are among  $v_1, \dots, v_{d-t}$ . The minimum weight in  $A^T$  is at least  $d-t$ .

The MacWilliams relations for  $A^T$  and  $B^{0 \neq T}$  determine the number of vectors of each of these weights uniquely in terms of  $n$ ,  $t$ ,  $q$ , and  $k$  via  $d-t$  equations

$$\sum_{j=v_1, \dots, v_{d-t}} \binom{n-t-j}{\mu} x_j = q^{n-t-k-\mu} \binom{n-t}{\mu} - \binom{n-t}{\mu}$$

$\mu = 0, 1, \dots, d-t-1$ , since the determinant of the coefficients is essentially Vandermonde. Since the weight distribution alone of a code determines that of the orthogonal code, again from MacWilliams [20], the weight distributions of  $A^T$  and  $B^{0 \neq T}$  are independent of the particular  $t$ -subset,  $T$ , chosen.

We now turn to the assertion concerning the  $t$ -designs which  $B$  yields. Suppose  $v$  is a weight in  $B$  satisfying  $v \leq w_0$ ,  $v \leq n-t$ . If  $b$  and  $b'$  are two vectors of  $B$  of weight  $v$  with their non-0 coordinates at the same coordinate set, then, since  $v \leq w_0$ ,  $b'$  is a scalar multiple of  $b$ . Consider the collection  $\mathcal{C}_v$  of coordinate  $v$ -subsets holding vectors of weight  $v$  in  $B$ . Let  $\mathcal{C}_v^c$  be the set of complements. By the Corollary to the Lemma, to show that  $\mathcal{C}_v^c$  is a  $t$ -design, it is enough to show that  $\mathcal{C}_v^c$  is. But, for a given  $t$ -set  $T$ , the number of subsets in  $\mathcal{C}_v^c$  containing  $T$  is  $\frac{1}{q-1}$  times the number of vectors in  $B^{0 \neq T}$  of weight  $v$ , and this number, by the above, is independent of which  $t$ -subset,  $T$ , is chosen.

The similar assertion for  $A$  is a bit more complicated to prove and we must apply the full Lemma. We start with  $w = d$ , which certainly satisfies  $w \leq v_0$ . As before, any two vectors of  $A$  of weight  $w$  held by the same coordinate-set are scalar multiples of one another. Let  $\mathcal{D}_w$  be the collection of coordinate  $w$ -subsets holding vectors of weight  $w$  in  $A$ . The number of subsets in  $\mathcal{D}_w$  containing a given  $t$ -subset  $T$  is  $\frac{1}{q-1}$  times the number of vectors of weight  $d-t$  in  $A^T$  and this, again, is independent of which  $t$ -subset,  $T$ , is chosen. We proceed by induction. So suppose we know the assertion of the theorem for  $w' < w$  where  $w \leq v_0$ . With  $\mathcal{D}_w$  as before, we know that the number of subsets in  $\mathcal{D}_w$  containing a given  $t$ -subset,  $T$ , is  $\frac{1}{q-1}$  times the number of vectors in  $A^T$  of weight  $w-t$  which come from vectors of weight  $w$  in  $A$ . Now, the total number of vectors of weight  $w-t$  in  $A^T$  is independent of  $T$  and it

follows immediately from the Lemma and the induction assumption that the number of vectors of weight  $w-t$  in  $A^T$  coming from vectors of weight less than  $w$  in  $A$  is independent of  $T$ . Thus,  $\mathcal{C}_w$  yields a  $t$ -design. This concludes the proof of the Theorem.

Applications of the Theorem. (1) Suppose  $A$  is a perfect code over  $GF(q)$  with minimum weight  $d$ . Then  $d$  is necessarily odd and the number of non-0 weights in its orthogonal complement is at most  $\frac{d-1}{2}$  [10,18]. Thus, we can take  $t = \frac{d+1}{2}$  and the Theorem yields  $t$ -designs. Cf. [6, Theorem 1].

MacWilliams [19] has shown that a necessary and sufficient condition for  $A$  to be perfect is that its orthogonal complement have precisely  $(d-1)/2$  non-0 weights. Our methods yield part of this result for  $GF(2)$ , namely, that a perfect linear code over  $GF(2)$  has at least  $(d-1)/2$  distinct non-0 weights in its orthogonal code: Let  $d = 2e+1$ . If there were fewer than  $e$  weights, the Theorem would yield an  $(e+2)$ -design from the minimum-weight vectors of the perfect code. In general there are  $(q-1)^{e+1} \binom{n}{e+1} / \binom{d}{e+1}$  such vectors in the code, because the parameters of the  $(e+1)$ -design are known (see [6]); this means that for the  $(e+2)$ -design  $\lambda$  would be  $(q-1)^e e / (n-e-1)$ . When  $q = 2$ , this cannot be an integer unless  $n = d$ , implying that the code is  $\{(0 \dots 0), (1 \ 1 \dots 1)\}$ , which does have exactly  $e$  distinct non-0 weights in its orthogonal code and which yields a trivial  $1; t-n-n$  design for all  $t$ . This proof cannot work in general, however, because the perfect  $(11,6)$  code over  $GF(3)$  (see Section 4) having  $d = 5$  yields a 3-design by the Theorem, but also yields in fact a 4-design, a  $1; 4-5-11$  Steiner system.

(2) We now derive well-known 5-designs and several new 5-designs by applying Theorem 4.2 to certain extended quadratic-residue codes.

a) 5-designs on 12 points. Consider the  $(12,6)$  code over  $GF(3)$ . This code is self-orthogonal and has vectors of weights 0, 6, 9, and 12 only. Thus for  $t = 5$  there is only one non-0 weight less than  $7 = 12-5$ , and  $d-t = 6-5 = 1$ . Therefore, the Theorem yields a  $\lambda; 5-6-12$  design as the 6-subsets of coordinate-places holding code-vectors. The weight-distribution shows now that  $\lambda = 1$ , because there are 4.66 weight-6 vectors and, for a  $\lambda; t-d-n$  design obtained in this way, we have  $\lambda \binom{n}{t} = \frac{N}{q-1} \binom{d}{t}$ , where  $N$  is the number of code-vectors of weight  $d$ .



For this code the weight-9 vectors also yield a design, but it is the trivial design since all 9-subsets arise in this way. This follows simply from the way  $\text{PSL}_2(11)$  acts.

The 1; 5-6-12 design is the well-known Steiner system having the Mathieu group  $M_{12}$  as automorphism group;  $M_{12}$  is also the automorphism group of the code [3, Section 4].

b) 5 designs on 24 points. Consider first the  $(24,12)$  code over  $\text{GF}(2)$ . This again is self-orthogonal, with non-0 weights 8, 12, 16, and 24. With  $t = 5$  we find three weights less than or equal to  $24-5 = 19$  and  $d-t = 3$ . Therefore, since  $q = 2$  we have 5-designs of 8-, 12-, and 16-subsets as follows:

$$1; 5 - 8 - 24$$

$$48; 5 - 12 - 24$$

$$78; 5 - 16 - 24$$

These  $\lambda$ 's are calculated from the weight-distribution, which appears in [23, p. 70]. Note that the first and third of these are complementary designs and the second of these is self-complementary, because of the presence of the all-1 vector in the code. Again, the 1; 5-8-24 design is the well-known Steiner system having the Mathieu group  $M_{24}$  as automorphism group, and the code also has  $M_{24}$  as automorphism group [3, Section 5].

Secondly, consider the  $(24,12)$  code over  $\text{GF}(3)$ . It is self-orthogonal with non-0 weights 9, 12, 15, 18, 21, and 24. For  $t = 5$  there are four weights below 19 and  $d-t = 4$ . Thus we get some new 5-designs from the 9-, 12-, and 15-subsets holding code-vectors, namely, the following:

$$6; 5 - 9 - 24$$

$$2^6 \cdot 3^2; 5 - 12 - 24$$

$$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13; 5 - 15 - 24$$

The first and third of these are not complementary, but we do not know whether the second design is self-complementary. The automorphism group of the 6;

5-9-24 design is not  $M_{24}$  but  $PSL_2(23)$ --hence the same for the code--a fact which will be proved later.

c) 5-designs on 48 points. The (48,24) code over  $GF(2)$  has 8 non-0 weights: 12, 16, 20, 24, 28, 32, 36, and 48. It is self-orthogonal and  $d = 12$ . Thus again  $d-5$  is the number of weights less than or equal to  $48-5$ , so the Theorem applies. From the weight-distribution we find the following parameters for the resulting designs:

$$\begin{aligned} 2^3; & \quad 5 - 12 - 48 \\ 3 \cdot 5 \cdot 7 \cdot 13; & \quad 5 - 16 - 48 \\ 2^4 \cdot 7 \cdot 17 \cdot 19; & \quad 5 - 20 - 48 \\ 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 227; & \quad 5 - 24 - 48 \end{aligned}$$

The code-vectors of weights 28, 32, and 36 form the 5-designs complementary to the first three of these. The last is self-complementary. We shall prove later that the automorphism group of each of these designs and of the (48,24) code is  $PSL_2(47)$ .

There are more 5-designs obtainable as the orbits of subsets of sets on which 5-fold transitive groups act; but, as we have said, some of the above 5-designs are not obtainable in this way. As an example of such a 5-design, consider a 12-subset  $U$  of the 24 points on which  $M_{24}$  acts such that the stability subgroup in  $M_{24}$  of  $U$  is  $M_{12}$ . Then the orbit of  $U$  under  $M_{24}$  is a 5-design on 24 points consisting of  $|M_{24}|/|M_{12}|$  12-subsets; it is a 48; 5-12-24 design with  $M_{24}$  as automorphism group.

(3) Finally, we apply the theorem to the construction of 3-designs.

a) 3-designs on 14 points. Consider the (14,7) quadratic-residue code over  $GF(4)$ . Here Theorem 4.1 tells us only that each weight class yields 2-designs; Theorem 4.2, however, produces 3-designs. The non-0 weights that appear are 6, 8, 12, 14. Since  $d-3 = 6-3 = 3$  and there are 3 non-0 weights less than or equal to  $14-3 = 11$ , we obtain 3-designs from the weight 6 vectors and the weight 8 vectors. The parameters are

$$5; \quad 3 - 6 - 14$$

$$2 \cdot 3^2 \cdot 7; \quad 3 - 8 - 14$$

b) 3-designs on  $2^k$  points,  $k$  odd. Finding designs and their parameters via Theorem 4.2 depends on knowing the weight distributions of the code and its orthogonal. Prange and Pless [24] have computed these distributions for all the cyclic codes of length 31. For example, several (31,21) cyclic codes over GF(2) yield the following designs and their complements (obtained by introducing a new coordinate equal the sum of all the others):

$$\lambda; \quad 3 - d - 32$$

4;	6
119;	8
1,464;	10
10,120;	12
32,760;	14
68,187;	16

(plus the complements of these).

The orthogonal code yields these designs:

$$2 \cdot 44; \quad 3 - 12 - 32$$

$$2 \cdot 136; \quad 3 - 16 - 32$$

$$2 \cdot 76; \quad 3 - 20 - 32$$

The designs of 16-clubs in both collections are self-complementary, and the designs of 12-clubs and 20-clubs from the orthogonal code are complements of each other. Also, the last three designs are each the union of two disjoint 2-designs.

These designs on 32 points are the first of an infinite class of 3-designs arising from a class of cyclic codes recently investigated by G. Solomon [28] and T. Kasami [16]. For each odd  $k$ , there are several  $(2^k - 1, 2k)$  cyclic codes with the following (non-0) weight-distribution:

<u>weight w</u>	<u><math>N_w</math> = number of code-vectors</u>
$2^{k-1}$	$(2^k - 1)(2^{k-1} + 1)$
$2^{k-1} + 2^{(k-1)/2}$	$(2^k - 1)(2^{k-2} - 2^{(k-3)/2})$
$2^{k-1} - 2^{(k-1)/2}$	$(2^k - 1)(2^{k-2} + 2^{(k-3)/2})$

One can show that the orthogonal code to any of these codes has minimum distance 5 (for it must be odd and at least 5; if 7 the code would be perfect!) Using the MacWilliams relations one could calculate the weight-distribution of the orthogonal and find the  $\lambda$ 's for the 3-designs obtained by introducing, as above, the new coordinate. For the  $(2^k, 2k+1)$  codes, the designs are of type  $2N_w; 3-w-2^k$ , with  $w$  and  $N_w$  as above.

(4) Examples for small n. Some 2- and 3-designs obtained from extended quadratic-residue codes are presented in the following table, along with the weight-distributions of the codes.  $N_w$  stands for the number of code-vectors of weight  $w$  in the indicated  $(n, n/2)$  code over  $GF(q)$ ; the entry  $\lambda; t$  in column  $w$  means that the code-vectors of weight  $w$  for that code yield a  $\lambda; t-w-n$  design.

$w =$	6	7	8	9	10	11	12	13	14		
$N_w$	330	396	495	1320	990	396	168			$n$	$q$
$\lambda; t$	10;3	21;3	42;3							12	4
$N_w$	440	528	2640	2640	5544	2640	1192			12	5
$\lambda; t$	10;3	21;3									
$N_w$	182	156	364	364	546	364	182	0	28	14	5
$\lambda; t$	15;2	18;2	56;2	72;2	135;2	110;2	trivial				
$N_w$	102		153		153		102				
$\lambda; t$	10;2		28;2							18	2
$\lambda; t^*$	5;3		21;3								

\*These 3-designs are obtained from the union of the two disjoint quadratic-residue codes, on which the 3-set transitive  $PGL_2(17)$  acts.

Other codes which might repay investigation are the  $(48,24)$  and  $(60,30)$ , both over  $GF(3)$ . In order for Theorem 4.2 to produce a 5-design, the minimum distances would have to be 15 and 18, respectively. The  $(72,36)$  code over  $GF(3)$  has a vector of weight 18, so the Theorem gives no information on that case; similarly, computations by Prange rule out the  $(\ell+1, (\ell+1)/2)$  codes over  $GF(2)$  for  $47 < \ell < 200$ . For a 5-design over  $GF(2)$ ,  $d$  must be greater than  $\ell/6$ , an unlikely result for large  $\ell$ .

## PART II

## SECTION 5

## AUTOMORPHISM GROUPS OF QUADRATIC-RESIDUE CODES AND 5-DESIGNS

Let  $\ell$  be an odd prime,  $p$  a prime distinct from  $\ell$ , and  $A$  and  $B$  the two finite  $\left(\ell+1, \frac{\ell+1}{2}\right)$  extended quadratic-residue codes over  $\mathbb{GF}(q)$  defined in Section 3, where  $q = p$  or  $p^2$  depending on whether or not  $p$  is a quadratic residue modulo  $\ell$ . Let  $G$  be the automorphism group of  $A$ . We know that  $\text{PSL}_2(\ell)$  is "contained in"  $G$  and that equality does not always obtain. This section will establish equality in certain cases.

We know, in general, that  $\text{PGL}_2(\ell)$  is not "contained in"  $G$ , since any element of  $\text{PGL}_2(\ell)$  not in  $\text{PSL}_2(\ell)$  will interchange  $A$  and  $B$ .

Let  $G_\infty$  be the stability group of  $\infty$ , i.e.,  $G_\infty = \{\sigma \in G; \sigma(\infty) = \infty\}$ .  $G_\infty$  is a transitive permutation group on  $\ell$  letters; it contains the permutations of the form  $x \mapsto ax+b$  where  $a \in \mathbb{GF}(\ell)^\times$  is a quadratic residue and  $b$  is an arbitrary element of  $\mathbb{GF}(\ell)$ . Call the group of all such permutations  $H$ . Then  $G = \text{PSL}_2(\ell)$  if and only if  $G_\infty = H$ . Moreover, the intersection of  $G_\infty$  with the full  $ax+b$  group is always  $H$  since  $G \cap \text{PGL}_2(\ell) = \text{PSL}_2(\ell)$ .

Now, given any transitive permutation group on  $\ell$  letters, any nontrivial normal subgroup is also transitive.

We shall also need the result that the subgroup  $H$  defined above has the group of all  $\sigma: x \mapsto ax+b$ , for all  $a \in \mathbb{GF}(\ell)^\times$  and all  $b \in \mathbb{GF}(\ell)$  as its normalizer in the symmetric group on  $\ell$  letters. One proves this by examining  $\pi^{-1} Z \pi$ , where  $\pi$  is in the normalizer and  $\pi(0) = 0$ ,  $\pi(1) = 1$ , and  $Z$  in  $H$  sends  $x$  to  $x+1$ .

It follows that a permutation group on  $\ell$  letters which contains  $H$  but not the full " $ax+b$ " group defined above is solvable if and only if it equals  $H$ . To see this one looks at a composition series of the given group,  $K$  say,  $K = K_0 \supset K_1 \supset \cdots \supset K_n \supset \{e\}$ . Now  $K_n$  is a simple transitive Abelian group on  $\ell$  letters, hence cyclic of order  $\ell$ . It is therefore permutation-isomorphic to the group generated by  $Z$  above. Since  $\langle Z \rangle$  is characteristic in the  $ax+b$

group and  $K_n$  is normal in  $K_{n-1}$ , the latter is isomorphic to a subgroup of the  $ax+b$  group. By induction so is  $K$ . Since  $K \supseteq H$  either  $K = H$  or  $(K:H) = 2$  and  $K$  is the full  $ax+b$  group, a case ruled out by hypothesis. We now have the following

**THEOREM 5.1.** If  $G$  properly "contains"  $PSL_2(\ell)$  then  $G_\infty$  is a nonsolvable transitive permutation group on  $\ell$  letters. Moreover, if  $\frac{\ell-1}{2} \geq 7$  and is prime, then  $G$  properly "contains"  $PSL_2(\ell)$  if and only if  $G$  is 5-fold transitive.

Proof. The first assertion follows from the above discussion. As for the second, the 5-fold transitivity of  $G$  immediately implies  $G \supset PSL_2(\ell)$ ; and the reverse implication is an immediate consequence of the nonsolvability of  $G_\infty$  and a deep result of Ito's [15, p. 151].

Parker and Nikolai have demonstrated the nonexistence of nonsolvable transitive permutation groups on  $\ell$  letters for  $\ell$  a prime such that  $\ell \neq 11, 23$ ,  $\ell \leq 4,079$ , and  $\frac{\ell-1}{2}$  prime. Therefore, we have

**COROLLARY 1.** For each Parker-Nikolai value of  $\ell$ , the codes  $A$  and  $B$  (for each  $p$ ) have  $PSL_2(\ell)$  as automorphism group. In particular, the 5-designs on 48 points have  $PSL_2(47)$  as automorphism group.

We remark that we first discovered that the group for  $\ell = 47$  is not 5-fold transitive by calculating and examining some of the weight-12 code-vectors.

**COROLLARY 2.** The  $(24,12)$  codes  $A$  and  $B$  over  $GF(3)$  and the associated 5-designs on 24 points have  $PSL_2(23)$  as automorphism group.

Proof. If the group were larger than  $PSL_2(23)$ , it would have to be the Mathieu group  $M_{24}$ , since that is the only 5-fold transitive group on 24 letters [13, p. 80].  $M_{24}$  is the automorphism group of the 1; 5-8-24 design, and if it also acted on the 6; 5-9-24 design associated with the minimum-weight vectors of the present code, then the subgroup  $M_0$  of  $M_{24}$  fixing each of 5 given points would have to permute the 6 9-subsets of the new design containing those 5 points.  $M_0$  has order 48 and it has two orbits on the remaining 19 points: one of length 3 and one of length 16. If we set down an incidence matrix of 6 rows and 24 columns for the 6 9-subsets mentioned above, then  $M_0$ , acting

on the columns, permutes the rows of the matrix. Ignoring the first 5 columns with all 1's, we find that each of the 3 columns in one orbit therefore has the same number, say  $x$ , of 1's; similarly, each of the 16 other columns has  $y$  1's. Therefore  $3x + 16y = 24$ ; but this is not solvable in integers since  $x \leq 6$ . Therefore  $M_{24}$  cannot act on the 6; 5-9-24 design, and the group of the latter is  $PSL_2(23)$ .

(One can see that  $M_0$  acts as claimed directly from the description of  $M_{24}$  in [31]; or, taking  $M_{24}$  as the automorphism group of the 5-8-24 Steiner system, assuming only the 5-fold transitivity and the order of  $M_{24}$ , one can prove that only the identity of  $M_{24}$  can fix each of 7 points not contained in an 8-set of the 1; 5-8-24 design. From this the action of  $M_0$  follows directly.)

These two Corollaries allow us to prove [7] that  $PSL_2(\ell)$  is the automorphism group of the Paley-Hadamard matrix of order  $\ell+1$  when  $(\ell-1)/2$  is prime,  $\ell \equiv -1 \pmod{12}$ , and  $23 \leq \ell \leq 4,079$ . The reason for the condition  $\ell = 12N - 1$  is that, since  $(3/\ell) = +1$ , we can regard the row-space of the matrix over  $GF(3)$  as an extended quadratic-residue code.

One should remark that the 6; 5-9-24 design coming from the (24,12) extended quadratic-residue code over  $GF(3)$  is suggestive of the design arising from a perfect code; a code is perfect if and only if the minimal weight vectors yield a  $(q-1)^e$ ;  $(e+1)$ - $d$ - $n$  design,\* where  $d = 2e + 1$ ; here we have  $\lambda = 6$  instead of 16, but otherwise the parameters are the same.

---

\*Proved in [6].



## PART II

## SECTION 6

## DISJOINT 5-DESIGNS

Each of the foregoing 5-designs arises from a finite extended quadratic-residue code. Since such codes occur in pairs, there are two 5-designs of each type; we ask whether they are disjoint. The answer is obviously yes for the designs arising from codes over  $GF(2)$ , because the codes are disjoint except for the all-1 vector. The codes over  $GF(3)$  are disjoint but the problem is that there are now two possible non-0 coefficients instead of only one; this means that a given set of coordinate-places might hold a vector from each code. We shall show, however, that this is not the case for the minimum-weight vectors of the codes in question.

**PROPOSITION.** Let  $\ell$  and  $(\ell-1)/2$  be primes, and let the minimum distance  $d$  in the finite extended quadratic-residue code of length  $\ell+1$  be less than  $(\ell-1)/2$ . Then the stability subgroup  $H$  in  $PSL_2(\ell)$  of a  $d$ -club has order  $h$  dividing  $d$  and  $\ell+1$ ; the orbits of  $H$  on the  $d$ -club are all of length  $h$ .

Proof. In  $PSL_2(\ell)$  the subgroup fixing 1 point has order  $\ell(\ell-1)/2$ . That fixing 2 points has order  $(\ell-1)/2$ . Since the latter is prime and any element in the stability subgroup is the product of cycles of lengths at most  $d$ , such an element cannot fix any points unless it is trivial. Therefore,  $H$  has only the trivial stability subgroup on any point of the  $d$ -club.

We shall apply this Proposition to some of the codes yielding 5-designs, retaining the notations  $H$  and  $h$ .

1) The (24,12) code over  $GF(3)$ . Here  $d$  is known to be 9. The number of 9-clubs in the 6; 5-9-24 design is  $N = 8 \cdot 11 \cdot 23$  and  $|PSL_2(23)| = 3N$ . Therefore  $H$  is nontrivial. Now it follows that  $h = 3$ , since  $3 = \gcd(9, 24)$ . Therefore  $PSL_2(23)$  is transitive on the 9-clubs of each of the two 5-designs, which means that the 5-designs are disjoint or equal. That the 5-designs are disjoint follows from the fact that we can produce two 9-clubs, one from each design, meeting in 7 points, which is impossible for two 9-clubs from the same design

(because it would imply the existence of a non-0 code vector of weight at most 7). The two 9-clubs arise from the code-polynomials  $(x-1)g(x)$  and its reverse,  $(x-1)g^*(x)$ , where  $g(x) g^*(x) = x^{22} + \dots + 1$  over  $GF(3)$ .

2) The (12,6) code over  $GF(3)$ . This case does not quite fit the Proposition, because  $d = 6$  is larger than  $(l-1)/2 = 5$ . However, we shall determine  $h$ . The 1; 5-6-12 design has  $N = 11 \cdot 12$  6-clubs and  $|PSL_2(11)| = 5 \cdot 11 \cdot 12$ . First of all,  $|H| \geq 5$ , and 11 does not divide  $|H|$  because every element has order at most 6. Let us take  $H$  to be the stability group of the 6-club  $\{1, 3, 4, 5, 9, \infty\}$  which arises from the obvious code-vector having 1 at each of these coordinate-places, which are the quadratic residues and  $\infty$ . The Galois group, sending  $i$  to  $3^ni \pmod{11}$ , fixes this 6-club, and therefore 5 divides  $|H|$ . Now if 2 divided  $|H|$ , Sylow theory would guarantee at least 6 subgroups of order 5 (since conjugation of  $(1\ 3\ 9\ 5\ 4)$  by  $(a\ b)(c\ d)(e\ f)$  would move the fixed point  $\infty$ ; there cannot be an element of order 2 which fixes any of the 6 points), hence at least 24 elements of order 5. Similarly there would be at least 5 elements of order 2, hence  $|H| \geq 30$ . Analogously, if 3 divided  $|H|$  we would find  $|H| > 30$ . The only divisors of  $|PSL_2(11)| = 5 \cdot 11 \cdot 12$  which are possible under the circumstances would be 60 and 30. 60 is impossible because the Sylow 2-subgroup would have to be the Klein 4-group, since no elements of order 4 could exist in  $H$ . But no two distinct elements of the form  $(a\ b)(c\ d)(e\ f)$  in  $\Sigma_6$  have another such as their product. Therefore,  $H$  would have to be 30, but we have already seen that such a group would have no room for elements of order 3. Therefore  $|H| = 5$  and  $PSL_2(11)$  is transitive on the 6-clubs of the 1; 5-6-12 design. Proposition 3.1 tells us now that the two designs of this type are disjoint or equal. To prove disjointness we examine the generator polynomials  $g(x)$  and the reverse  $g^*(x)$ , of degree 5. The weights of these are at most 6, and if 6 then the infinite coordinate would have to be 0 (by Theorem 3.3), contradicting that  $x-1$  does not divide either. Therefore each has weight 5 and gives a non-0 coordinate at  $\infty$ . These are then two different 6-clubs meeting in 5 places, hence not members of the same 1; 5-6-12 design (Cf. [14; p. 774]).

Thus we have shown that each of the 5-designs of Section 4 for the minimum-weight vectors exist in disjoint pairs. This means in particular that the union of the two designs is a 5-design with  $\lambda$  doubled.\*

A related question is that of the action  $\text{PSL}_2(\ell)$  on the  $d$ -clubs, where  $d$  is the minimum weight in the code. We have already shown that  $\text{PSL}_2(\ell)$  is transitive on the  $d$ -clubs for  $\ell = 11$  and  $\ell = 23$  over  $\text{GF}(3)$ . The question naturally arises for the other two codes producing 5-designs.

Consider the  $(24, 12)$  code over  $\text{GF}(2)$ . Here  $d = 8$  and the number of minimum-weight vectors is  $759 = 3 \cdot 11 \cdot 23 = N$ . The order of  $\text{PSL}_2(23)$  is  $8N$ . From the Proposition we know that  $H$  is nontrivial and has order dividing 8. But  $|H| \geq 8$  by an orbit-count. Therefore  $|H| = 8$  and  $\text{PSL}_2(23)$  is transitive on the 8-clubs of the two 1; 5-8-24 Steiner systems.

The  $(48, 24)$  code over  $\text{GF}(2)$  is harder to analyze. All we can tell from what we have so far is that the order  $h$  of the stability-subgroup of a 12-club satisfies  $h \geq 3$  and  $h|12$ ;  $\text{PSL}_2(47)$  is transitive on the 12-clubs if and only if  $h = 3$ , since there are  $N = 16 \cdot 23 \cdot 47$  12-clubs and  $|\text{PSL}_2(47)| = 3N$ .

---

\*We announced this result for two 5-designs, those associated with the Mathieu groups  $M_{12}$  and  $M_{24}$ , in [4].

## REFERENCES

1. E. F. Assmus, Jr., and H. F. Mattson, Jr., "Cyclic Codes," Summary Scientific Report #4, Air Force Cambridge Research Laboratories, AFCRL-65-332, April 28, 1965.
2. E. F. Assmus, Jr., and H. F. Mattson, Jr., "Cyclic Codes," Final Report, Air Force Cambridge Research Laboratories, AFCRL-66-348, April 28, 1966.
3. E. F. Assmus, Jr., and H. F. Mattson, Jr., "Perfect Codes and the Mathieu Groups," Archiv der Math., vol. XVII, pp. 121-135; 1966.
4. E. F. Assmus, Jr., and H. F. Mattson, Jr., "Disjoint Steiner Systems Associated with the Mathieu Groups," Bull. AMS, vol. 72, pp. 843-845; 1966.
5. E. F. Assmus, Jr., and H. F. Mattson, Jr., "On the Number of Inequivalent Steiner Triple Systems," J. Comb. Theory, vol. 1, pp. 301-305; 1966.
6. E. F. Assmus, Jr., and H. F. Mattson, Jr., "On Tactical Configurations and Error-Correcting Codes," J. Comb. Theory, vol. 2, pp. 243-257, 1967.
7. E. F. Assmus, Jr., and H. F. Mattson, Jr., "On the Automorphism Groups of Paley-Hadamard Matrices," Proceedings of the Conference on Combinatorial Mathematics and Its Applications, University of North Carolina, April 1967; to appear.
8. R. C. Bose, "On Some Connections Between the Design of Experiments and Information Theory," Bulletin of the International Statistical Institute, vol. 38, pp. 257-271; 1961.
9. A. M. Gleason, private communications. (Many of these are recorded in [1] and [2].)
10. M. J. E. Golay, "Binary Coding," IRE Trans. on Information Theory, vol. IT-4, pp. 23-28; 1954.
11. J. H. Griesmer, "A Bound for Error-Correcting Codes," IBM J. Res. Develop. vol. 4, pp. 532-542; 1960; MR23B(1962), #B3081.
12. M. Hall, Jr., "Note on the Mathieu Group  $M_{12}$ ," Archiv der Math., vol. XIII, pp. 334-340; 1962.
13. M. Hall, Jr., The Theory of Groups, Macmillan, New York; 1959.
14. D. R. Hughes, "t-Designs and Groups," Amer. J. Math., vol. 87, pp. 761-778; 1965.
15. N. Ito, "Transitive Permutation Groups of Degree  $p = 2q+1$ ,  $p$  and  $q$  Being Prime Numbers, III," Trans. AMS, vol. 116, pp. 151-166; 1965.

16. T. Kasami, "Weight-Distribution of Bose-Chaudhuri-Hocquenghem Codes," Report R-317 Coordinated Science Laboratory, University of Illinois, Urbana, Illinois, August 1966. Proceedings of Conference on Combinatorial Mathematics and Its Applications, University of North Carolina, April 1967; to appear.
17. T. Kasami and S. Lin, "Some Codes Which Are Invariant Under a Doubly-Transitive Permutation Group and Their Connection with Balanced Incomplete Block Designs," AFCRL-66-142, Scientific Report No. 6, January 28, 1966, AF19(628)-4379.
18. S. P. Lloyd, "Binary Block Coding," Bell Sys. Tech. J., vol. 36, pp. 517-535; 1957. MR 19 (1958), p. 465.
19. F. J. MacWilliams, Ph.D. dissertation, Harvard University, 1962?, unpublished.
20. F. J. MacWilliams, "A Theorem on the Distribution of Weights in a Systematic Code," Bell Sys. Tech. J., vol. 42, pp. 79-94; 1963; MR 26 (1963) #7462.
21. L. J. Paige, "A Note on the Mathieu Groups," Can. J. Math., vol. 9, pp. 15-18; 1956.
22. E. T. Parker and P. J. Nikolai, "A Search for Analogues of the Mathieu Groups," Math. Tables Aids Comput., vol. 12, pp. 38-43; 1958, MR 21 #450.
23. W. W. Peterson, Error-Correcting Codes, M.I.T. Press and John Wiley and Sons, Inc., New York; 1961.
24. Vera Pless and E. Prange, "Weight Distributions of all Cyclic Codes in a Vector Space of Dimension 31 Over GF(2)," AFCRL memo, September 1962.
25. E. A. Prange, "Codes Equivalent Under the Projective Group (III)," AFCRL unpublished memorandum, July 10, 1962.
26. R. Silverman, "A Metrization for Power-Sets with Applications to Combinatorial Analysis," Can. J. Math., vol. 12, pp. 158-176; 1960; MR 25 #4019.
27. R. C. Singleton, "Maximum Distance q-nary Codes," IEEE Trans. on Information Theory, vol. IT-10, pp. 116-118; 1964.
28. G. Solomon, "Tri-Weight Cyclic Codes," Jet Propulsion Lab., SPS 37-41.
29. G. Solomon and J. J. Stiffler, "Algebraically Punctured Cyclic Codes," Inf. and Control, vol. 3, pp. 170-179; 1965; MR 30 (1965) #5847.
30. P. J. Turyn, "A Theorem of Gleason and Pierce," Sylvania memo, December 1966. Also Part XI of this report.
31. E. Witt, "Die 5-fach transitiven Gruppen von Mathieu," Abhandlungen aus dem Math. Sem. Hansischen Universitat, vol. 12, pp. 256-264; 1938.

## PART III

## ON THE AUTOMORPHISM GROUPS OF PALEY-HADAMARD MATRICES\*

For a prime\*\* of the form  $\ell = 4N-1$ , the Paley-Hadamard matrix of order  $\ell + 1$  is defined as the  $(\ell+1) \times (\ell+1)$  matrix of  $+1$ 's and  $-1$ 's with the first row and first column all  $+1$ 's; the second row is defined to be  $-1$  at  $0$  and at the quadratic nonresidues modulo  $\ell$  and  $+1$  elsewhere. The columns are indexed as  $(\infty; 0, 1, 2, \dots, \ell-1)$ . The remaining  $\ell - 1$  rows are defined to be the cyclic shifts of the "finite part" of the second row.

The automorphism group of a Hadamard matrix is defined as the group of  $(\ell+1) \times (\ell+1)$  monomial matrices (with entries  $0, \pm 1$ ) modulo  $\{\pm I\}$ ,  $I$  being the identity, which acts on the right on the Hadamard matrix in such a way that the result is the original Hadamard matrix except for a permutation of rows and a possible change of sign of some rows.

A monomial matrix is of course the product of a diagonal matrix and a permutation matrix. The mapping which sends each element of the above automorphism group to the associated permutation matrix is an isomorphism, as one can easily verify. Because we are concerned with the permutation group which is the image of this isomorphism, we shall speak of the automorphism group of the matrix as being, or being contained in, this or that permutation group.

It is known ([4],[1]) that when  $\ell = 11$ , the automorphism group is the Mathieu group  $M_{12}$ . What we prove here is the following

THEOREM. When  $\ell$  is a prime of the form  $12N-1$  with  $6N-1$  also prime and  $23 \leq \ell \leq 4,079$ , then the automorphism group  $G$  of the Paley-Hadamard matrix of order  $\ell + 1$  is the projective unimodular group  $PSL_2(\ell)$ .

$PSL_2(\ell)$  is the group of all  $2 \times 2$  matrices with determinant  $1$ , modulo  $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , over  $GF(\ell)$ . It is a 2-fold transitive permutation group on the projective line.

---

\* Presented at the Conference on Combinatorial Mathematics and its Applications, University of North Carolina, Chapel Hill, North Carolina, April 10-April 14, 1967.

\*\* In fact  $\ell$  could be a prime power.

Proof of the Theorem. Hall [4] has proved that the automorphism group of a Paley-Hadamard matrix contains  $\text{PSL}_2(\ell)$ . Consider the rows of the matrix to be vectors over  $\text{GF}(3)$ . Their linear span is contained in\* a so-called extended  $(\ell+1, (\ell+1)/2)$  quadratic-residue code over  $\text{GF}(3)$ , of dimension  $(\ell+1)/2$ , of which there are two, here called A and B. Let A be the row-space of the matrix. Then G leaves A invariant. The group  $\text{PSL}_2(\ell)$  acts on both codes together, and any element of  $\text{PGL}_2(\ell)$  not in  $\text{PSL}_2(\ell)$  maps A onto B and B onto A. Also,  $A \cap B = 0$ . ([3],[8]) This motivates our choice of  $\ell$  so that  $(3/\ell) = +1$ ; otherwise the row-space has dimension  $\ell$ .

Case 1.  $23 < \ell \leq 4,079$ . The subgroup of  $\text{PSL}_2(\ell)$  which fixes the "infinite" coordinate of the code (or column of the Paley-Hadamard matrix) is the group sending  $x$  to  $a^2 x + b$  for  $a, b \in \text{GF}(\ell)$  with  $a \neq 0$ . It is transitive on the "finite" coordinates (columns). Nikolai and Parker [7] show, however, that there are no transitive nonsolvable groups on  $\ell$  letters. Let  $G_\infty$  be the subgroup of G fixing the column  $\infty$ . Then  $G_\infty$  is solvable, and by elementary arguments one sees that  $G_\infty$  is contained in the " $ax + b$ " group, which sends  $x$  to  $ax + b$  for all  $a, b \in \text{GF}(\ell)$  with  $a \neq 0$ . But  $G_\infty$  contains the " $a^2 x + b$ " group, and if  $G_\infty$  were equal to the  $ax + b$  group, then G would not leave A invariant but would contain elements mapping A onto B. Therefore  $G_\infty$  is the  $a^2 x + b$  group and  $G = \text{PSL}_2(\ell)$ .

Case 2.  $\ell = 23$ . Here there is of course a nonsolvable group, namely the Mathieu group  $M_{23}$ , and hence there is the possibility that  $M_{24}$  could be the automorphism group of the Paley-Hadamard matrix of order 24, since  $M_{23}$  is contained in the 5-fold transitive group  $M_{24}$  as the stability subgroup of a point. Furthermore,  $M_{24}$  is the only 5-fold transitive group on 24 letters [5,p.80].

Itô [6] proves that if  $\ell$  and  $(\ell-1)/2$  are primes with  $\ell > 11$ , then a nonsolvable, transitive permutation group on  $\ell$  letters is 4-fold transitive. It follows from this result that if G for  $\ell = 23$  is larger than  $\text{PSL}_2(23)$ , then it is 5-fold transitive and therefore is  $M_{24}$ . We now sketch a proof that  $M_{24}$  is not the automorphism group.

---

\*The relation is equality but we only need the inclusion.

$M_{24}$  is best regarded as the automorphism group of a certain tactical configuration, namely, a Steiner system of type 5-8-24. This configuration is a collection  $D$  of 8-subsets of a set of 24 points such that every 5-subset of the 24-set is contained in exactly one element of  $D$ . Witt [9] proved that such a configuration is unique (up to action by the symmetric group  $\sum_{24}$  on the 24 points) and that the subgroup of  $\sum_{24}$  which permutes the elements of  $D$  among themselves is a 5-fold transitive group of order  $48 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20$ . This group is, by definition, the automorphism group of the 5-8-24 Steiner system; and, since Witt, this is the most commonly used definition of  $M_{24}$ .

For our proof we need some simple properties of  $M_{24}$ . From the 5-fold transitivity it follows that the subgroup  $G_0$  of  $M_{24}$  which fixes each of 5 points has order 48. We need to know the action of  $G_0$  on the remaining 19 points.

LEMMA.  $G_0$  has two orbits--one of length 3 and one of length 16--on the remaining 19 points.

Proof. The 5 fixed points of  $G_0$  are contained in a unique 8-set belonging to  $D$ . Therefore  $G_0$  acts on the remaining 3 points  $X$  of the 8-set and on the other 16 points  $Y$ . To see that these actions are transitive one can refer to [9], where an explicit description of  $G_0$  as  $3 \times 3$  matrices over  $GF(4)$  acting on the projective space of 21 points over  $GF(4)$  is given.

It is also possible to prove transitivity from the definition and properties of  $M_{24}$  listed above. One proves that only the identity element of  $M_{24}$  can fix 7 points not contained in an 8-set belonging to  $D$ . (One sees this by picking pairs of 5-subsets of the 7 points which meet in 3 points. These give rise to pairs of 3-subsets outside the 7 meeting in 1 point, which must be also fixed. Continuing, one gets all points fixed.) Then consider the stability subgroup  $G_1$  in  $G_0$  of a point from the 16-set  $Y$ .  $G_1$  must have order at least 3, but no nontrivial element  $\sigma$  of  $G_1$  can fix any more points. This means, in particular, that  $\sigma$  is a 3-cycle on the 3 points of  $X$ , and thus  $G_0$  is transitive on  $X$ . Moreover,  $\sigma^3$  is the identity on 9 points and therefore  $\sigma^3 = 1$ . Since now every nontrivial element of  $G_1$  has order 3,  $G_1$  must have order 3 since  $G_0 = 3 \cdot 16$ . Therefore  $G_0$  is transitive on  $Y$  also.



We use this Lemma in the situation arising from the code generated by the rows of the Paley-Hadamard matrix over  $GF(3)$ . This code is the whole extended quadratic-residue code  $A$  of type  $(24,12)$  over  $GF(3)$ , because the latter is the sum of  $\alpha(1\ 1\ 1\cdots 1;1)$ ,  $\alpha = 0, \pm 1$ , and the irreducible  $(24,11)$  extended quadratic-residue code. We have proved [2] that  $A$  has the following properties.

**PROPOSITION.** The minimum distance in  $A$  is 9; the 9-subsets of coordinate-places of  $A$  holding minimum-weight code-vectors form a tactical configuration of type 6; 5-9-24. (Thus every 5-subset is in precisely 6 of the given 9-subsets.)

We use our Lemma to show that  $M_{24}$  cannot act on this design, as it would certainly do if it were the automorphism group of the matrix. Consider a given 5-subset of the 24-set. There are the two subsets  $X$  and  $Y$ , of cardinalities 3 and 16, respectively, on which  $G_0$  of the Lemma is transitive. The 6 different 9-subsets containing the given 5-subset of the new design have  $6(9-5) = 24$  points distributed with multiplicities among the remaining 19 points. Arrange them in a  $6 \times 19$  incidence matrix. If  $M_{24}$  acts, then  $G_0$  acting on the columns must permute the 6 rows. By the Lemma, there are the same number of these incidences, say  $x$ , in each of the three columns determined by  $X$ , and there are  $y$  in each column determined by  $Y$ . This means  $3x + 16y = 24$ , but since  $x \leq 6$  this is not solvable in integers. Therefore  $M_{24}$  does not act on the 6; 5-9-24 design. Hence the automorphism group of the code is  $PSL_2(23)$ , and the same for the Paley-Hadamard matrix.

As we showed in [1], the row space generated over  $GF(3)$  by the rows of the Paley-Hadamard matrix of order 12 yields the 5-6-12 Steiner system (a "5-design") of which  $M_{12}$  is the automorphism group. Thus, for order 24 the 5-design remains but the group is no longer large. We do not yet know whether the order 48 Paley-Hadamard matrix yields a 5-design, but there is a possibility that it will.

Acknowledgment. Our interest and what knowledge we have of these matters owes much to continued conversations with A. M. Gleason and Richard Turyn.

Added After the Conference. On the above result for  $\ell = 23$ , M. Hall has informed us that Gordon Keller has shown that  $M_{24}$  cannot act on any Hadamard matrix of order 24.

In [10] is indicated, in effect, that the subgroup of  $G_\infty$  (for  $\ell = 23$ ) which acts without any signs, thus fixing row  $\infty$  as well as column  $\infty$ , is the " $a^2 x + b$ " group; but it is not clear how to proceed from this subgroup to  $G_\infty$ .

#### REFERENCES

1. E. F. Assmus, Jr. and H. F. Mattson, Jr., "Perfect Codes and the Mathieu Groups," Archiv der Math., vol. XVII, pp. 121-135; 1966.
2. E. F. Assmus, Jr. and H. F. Mattson, Jr., to appear.
3. A. M. Gleason, private communications, presented in [11].
4. M. Hall, Jr., "Note on the Mathieu Group  $M_{12}$ ," Archiv der Math., vol. XIII, pp. 334-340; 1962.
5. M. Hall, Jr., The Theory of Groups, MacMillan, N. Y.; 1959.
6. N. Ito, "Transitive permutation groups of degree  $p = 2q+1$ ,  $p$  and  $q$  being prime numbers, III" Transactions AMS, vol. 116, pp. 151-166; 1965.
7. E. T. Parker and P. J. Nikolai, "A Search for Analogues of the Mathieu Groups," Math. Tables Aids Comput., vol. 12, pp. 38-43, MR 21 #450; 1958.
8. E. A. Prange, "Codes Equivalent Under the Projective Group (III)," AFCRL 10, July 1962, unpublished memorandum; also presented in [11].
9. E. Witt, "Die 5-fach transitiven Gruppen von Mathieu." Abhandlungen aus dem Math. Sem. Hansischen Universitat. vol. 12, pp. 16-264; 1938.
10. J. A. Todd, "A Combinatorial Problem," J. Math Physics, vol. 12, pp. 321-333; 1933.
11. E. F. Assmus, Jr. and H. F. Mattson, Jr., "Cyclic Codes," AFCRL-65-322; April 28, 1965.

## PART IV

## SOME REMARKS ON AUTOMORPHISM GROUPS OF HADAMARD MATRICES

In this section we shall prove some assorted facts about the automorphism groups of Hadamard matrices. An Hadamard matrix  $H$  has entries  $\pm 1$  and satisfies  $HH' = nI$   $n$  = order of  $H$ ,  $H' =$  transpose of  $H$ . ( $n=1,2$  or  $4t$ ). A generalized Hadamard matrix has entries  $m$ -th roots of 1,  $m > 2$ , and satisfies  $HH^* = nI$ ,  $H^* = \overline{H'} =$  complex conjugate of  $H'$ .

Two Hadamard matrices are equivalent if  $H_1 = M_1 H M_2$ ,  $M_i$  monomial matrices, i.e.,  $M_i = P_i D_i$ , with  $P_i$  permutation matrices and  $D_i$  diagonal matrices (with  $\pm 1$  or  $m$ -th roots on the diagonal). The group of automorphisms of  $H$  is the set of pairs of monomial matrices  $M_1, M_2$  such that  $M_1^* H M_2 = H$ , modulo the center, the set of all  $(cI, cI)$ .  $M_1$  determines  $M_2$  uniquely and vice versa, and  $P_i$  determines  $D_i$ , modulo the center.

In [1], Hall remarks that there is only one Hadamard matrix of order 12 up to equivalence (this is also easily checked for  $n = 1, 2, 4, 8$ ; for  $n = 16$  there are five such matrices). We shall first prove this fact, in such a way that it will be obvious that the group of this matrix is exactly 5-fold transitive as a permutation group on the rows. We shall denote by  $H_2$  the matrix

$$\begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

Let  $H$  be any Hadamard matrix of order 12, and pick out any 5 rows in definite order. We shall reduce the matrix to a canonical form, and these five rows into the first five rows of our matrix.

It is clear that, if  $n > 2$ , any first three rows of an Hadamard matrix can be reduced to the form

$$\begin{array}{cccc} + & + & + & + \\ + & + & - & - \\ + & - & + & - \end{array}$$

by a suitable multiplication of the columns by  $\pm 1$  and permutation of the columns, (where  $+$  indicates a row of  $\frac{n}{4}$  plus ones!). These three rows are like the first three rows of  $H_2^{(2)}$  ( $H_2^{(n)}$  = Kronecker product of  $H_2$  with itself  $n$  times), with the interpretation of  $+$  as a row of  $+1$ 's of appropriate size. We now note:

LEMMA. If the first  $2^m$  rows of  $H$  coincide with  $H_2^{(m)}$ , then  $H$  is equivalent to  $H_2^{(m)}$  or  $2^{m+1}$  divides  $n$  = order of  $H$ .

Assume  $n > 2^m$ , let  $t = n2^{-m}$ , and let  $(S_1, \dots, S_{2^m}) = S$  be the vector of sums of any row past the first  $2^m$ .  $\left( S_1 = \sum_{i=1}^t x_i, S_2 = \sum_{i=t+1}^{2t} x_i, \text{ etc.}, \text{ where } (x_1, \dots, x_n) \text{ is a row of the Hadamard matrix} \right)$ . Then the condition that this row be orthogonal to the first  $2^m$  rows implies

$$S H_2^{(m)} = 0$$

and since  $H_2$  is nonsingular  $S = 0$ , thus  $S_1 = 0$  and, therefore,  $t$  is even.

Returning to the matrix of order 12, the Lemma implies that we cannot have four rows which reduce to

$$\begin{array}{cccc} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{array}$$

(where we have interchanged rows 2 and 3).

Consider any further row, and as before let  $S_1, \dots, S_4$  be the sums of three consecutive entries. Orthogonality to the first three rows implies

$$S_1 + S_2 + S_3 + S_4 = 0$$

$$S_1 + S_2 - S_3 - S_4 = 0$$

$$S_1 - S_2 + S_3 - S_4 = 0$$

or  $S_1 = -S_2 = -S_3 = S_4$ . We have just noted that  $S_1 = \pm 3$  is impossible; thus  $S_i = \pm 1$  for all further rows.

Any further row looks like

- + + + - - + - - - + +

(after suitable change of sign and permutation of columns within the four blocks of three each.) Thus, within each block of 3 columns, two rows have dot product +3 or -1; therefore any pair coincides in exactly one block of 3. We now reduce our matrix of order 12 by permuting the three blocks of four columns so that the fourth and fifth rows coincide in the first block of 3 columns. This may involve changing the signs of the second and third rows. Now permute the columns of the second, third, and fourth block so that the first five rows take the form

+ + + + + + + + +  
 + + + + + + - - - - - -  
 + + + - - - + + + - - -  
 - + + + - - + - - - + +  
 - + + - + - - + - + - +

The only column permutation that may be performed now is the interchange of the second and third columns.

Each row past the third can be identified by a quadruple  $(i, j, k, \ell)$  where  $1 \leq i, j, k, \ell \leq 3$  and each denote the position within the block of three of the "unusual" element (-1 if the sum of three is +1, +1 otherwise). We have reduced the first three rows to the form

(1,1,1,1)

(1,2,2,2)

The orthogonality condition states that any two quadruples coincide in exactly one position. It can be immediately verified that there are at most 9 such quadruples, and, given the first two, the  $9 \times 4$  array can be constructed in exactly two ways; we use the interchange of the first two columns to normalize it to a unique array ((1,3,3,3) must be a fourth row, and (-,2,3,1) must occur: we require, e.g., that (2,2,3,1) occur rather than (3,2,3,1)).

We remark that the  $9 \times 4$  array is the array constructed from a projective plane of order 3 in a standard fashion: a projective plane of order 3 is equivalent to a pair of orthogonal  $3 \times 3$  Latin squares, and such a pair is equivalent to the  $9 \times 4$  array. The array is constructed as the set of all  $(i, j, x_{ij}, y_{ij})$   $1 \leq i, j \leq 3$ , with  $[x_{ij}]$ ,  $[y_{ij}]$  the two Latin squares.

We have now shown that any Hadamard matrix of order 12 can be reduced to a unique form, and further that the automorphism group is exactly 5-fold transitive. It is known that such a group is unique, the Mathieu group  $M_{12}$  (see [1]).

Since we have such a simple construction of the group  $M_{12}$ , it is tempting to look for an Hadamard matrix of order 24 on which  $M_{24}$  acts. It follows from the results of Assmus and Mattson that the Paley-Hadamard matrix constructed from the quadratic residues mod 23 admits only the obvious group of automorphisms,  $PSL(2,23)$ , (of order much smaller than the order of  $M_{24} = \frac{24!}{19!} \cdot 48$ ).

**THEOREM.** There is no generalized Hadamard matrix  $H$  with entries 24-th roots of 1 on whose rows  $M_{24}$  acts faithfully.

Proof.  $M_{24}$  contains a 23 cycle. If a matrix  $H$  existed on whose rows  $M_{24}$  acted faithfully, we could take a matrix equivalent to  $H$  such that the given element of order 23 acted without signs, i.e., left the first row and column fixed, and the elements of the first row and column could be reduced to +1's.

The columns can be arranged so that the action of the cycle is  $(1, 2, \dots, 23)$  on both the rows and the columns. Then if  $x_1, \dots, x_{23}$  denote the elements of the second row, exclusive of the +1 in the first column, the orthogonality relations state that

$$1 + \sum_{i=1}^{23} x_i \bar{x}_{i+j} = 0 \quad \text{for } j \neq 0$$

and, of course,  $\sum x_i \bar{x}_i = 23$ . These equations are clearly equivalent to

$$\left( \sum x_i \zeta^i \right) \left( \sum x_i \zeta^{-i} \right) = 24 \quad \zeta^{23} = 1, \zeta \neq 1$$

$$\text{or } \left| \sum x_i \zeta^i \right| = 2\sqrt{6}$$

We must also have  $1 + \sum x_i = 0$  to have the first row of the matrix orthogonal to all the others.

Modulo 23, 2 generates the quadratic residues, whereas 3 is primitive ( $2^5 = 3^2$ , and thus  $2 = 2^{45} = 3^{18}$ ). Therefore, the number 3 remains prime in  $Q(\zeta)$ , and 2 factors into two prime ideals in  $Q(\zeta)$ . Now the automorphism  $\sigma(x) = x$ ,  $\sigma(\zeta) = \zeta^2$ ,  $x$  in the field of 24-th roots of 1, will leave invariant the prime ideals dividing 2 and 3 in the field of  $(23 \cdot 24)$ -th roots of 1. Thus  $\sum x_i \zeta^i = w \left( \sum x_i \zeta^{2i} \right)$  with  $w$  a root of 1, since  $w$  is an integer and  $\left| \sum x_i \zeta^i \right| = \left| \sum x_i \zeta^{2i} \right| = 2\sqrt{6}$ , so  $|w| = 1$ . Let  $\bar{w} = w_1 \zeta^a$  with  $w_1$  a 24-th root of 1. Let  $A = \sum x_i \zeta^i$ . Then

$$\sigma(A) = w A$$

$$\sigma^2(A) = \sigma(w) w A = w_1^2 \zeta^{2a+a} A$$

$$\sigma^{11}(A) = w_1^{11} \zeta^{2047a} A = w_1^{11} A$$

But since  $\sigma^{11}$  is the identity,  $w_1^{11} = 1$ , and thus  $w_1 = 1$ .

$$\sigma(A) = \zeta^2 A$$

$$\sigma(\zeta^{-a} A) = \zeta^{-2a+a} A = \zeta^{-a} A$$

Thus  $\sum x_i \zeta^{i-a}$  is invariant under  $\sigma$ , and if we replace each row by a translate, (take a new form of our matrix) we can assume  $\sum x_i \zeta^i$  is invariant under  $\sigma$ .

Thus

$$\sum x_i \zeta^i = \sum x_i \zeta^{2i}$$

or

$$\sum (x_{2j} - x_j) \zeta^j = 0$$

We have a relation with first coefficient zero, and since  $\zeta$  is of degree 23 over the field of 24-th roots of 1,  $x_{2j} = x_j$  for all  $j$ . Therefore

$$A = \sum x_i \zeta^i = x_0 + x_1 \eta + x_{-1} \bar{\eta}, \quad \eta = \sum \zeta^r, \quad r \text{ running over all the residues.}$$

$\eta + \bar{\eta} = -1$ ,  $\eta \bar{\eta} = 6$ .  $\left| (x_1 - x_0) \eta + (x_{-1} - x_0) \bar{\eta} \right| = 2\sqrt{6}$ . The condition  $1 + \sum x_i = 0$  implies  $1 + x_0 + 11(x_1 + x_{-1}) = 0$ , and thus  $x_0 = -1$ ,  $x_1 = -x_{-1}$

Thus

$$\begin{aligned} 24 &= 6 \left\{ (x_1 - 1)(\bar{x}_1 - 1) + (x_1 + 1)(\bar{x}_1 + 1) \right\} \\ &\quad + (x_1 - 1)(-\bar{x}_1 - 1) \eta^2 + (\bar{x}_1 - 1)(-x_1 - 1) \bar{\eta}^2 \\ &= 24 + (\bar{x}_1 - x_1) \eta^2 + (x_1 - \bar{x}_1) \bar{\eta}^2 \\ &= 24 + (\bar{x}_1 - x_1) (\eta^2 - \bar{\eta}^2) \end{aligned}$$



Since  $\eta^2 - \bar{\eta}^2 \neq 0$ , we must have  $x_1 = \bar{x}_1$  which implies  $x_1 = \pm 1$ , and the matrix reduces to the Paley-Hadamard matrix, which, however, does not admit  $M_{24}$  as a group of permutations of the rows. We have shown that any generalized Hadamard matrix with 24-th roots of 1 as entries which has a group of automorphisms of order 23 is equivalent to the Paley-Hadamard matrix.

There is another obvious Hadamard matrix of order 24,  $H_2 \times H_{12}$  (Kronecker product,  $H_{12}$  the Hadamard matrix of order 12). We know that  $H_2 \times H_{12}$  cannot admit  $M_{24}$  as a group of automorphisms. However, it does have a relatively large group, and, by the Assmus-Mattson result, we can conclude that it is not equivalent to the Paley-Hadamard matrix.

THEOREM. Let  $G_i$  be the automorphism group of  $A_i$ ,  $A_i$  an Hadamard matrix,  $i = 1, 2$ . Then  $G_1 \times G_2$  is included in the group of  $A_1 \times A_2$ .

Let  $N_i A_i M_i = A_i$ ,  $i = 1, 2$ . Then  $(N_1 \times N_2)(A_1 \times A_2)(M_1 \times M_2) = (N_1 A_1 M_1) \times (N_2 A_2 M_2) = A_1 \times A_2$ , so  $G_1 \times G_2$  is a subgroup of the automorphism group of  $A_1 \times A_2$  in a natural way. Since  $H_2$  has an automorphism group of order 4, the automorphism group of  $H_2 \times H_{12}$  is of order  $\geq 4 \cdot \frac{12!}{5!}$ .

It is natural to ask whether  $G_1 \times G_2$  is actually the whole group of automorphisms of  $A_1 \times A_2$ . A counterexample is furnished by the matrix  $H_2 \times H_2$ : the automorphism group of  $H_2^{(n)}$  is of order  $2^{2n}(2^n-1)(2^n-2)\dots(2^n-2^{n-1})$ , since with the first row fixed, the group is the group  $x \rightarrow Ax+y$ ,  $A$  a nonsingular transformation of the  $n$ -dimensional vector space over  $GF(2)$ .

On the other hand, the group of a Kronecker product cannot be too large:

THEOREM. If  $A$  and  $B$  are Hadamard matrices, the group of  $A \times B$  cannot be 4-fold transitive on the rows unless  $A \times B = H_2^{(2)}$ .

Take the matrices  $A$  and  $B$  so that the first two rows of each are

+ +

+ -

Then  $A \times B$  has four rows which look like  $H_2^{(2)}$ ; an automorphism which fixes the first three of these clearly fixes the fourth.

In [1] Hall proved that the group  $PSL(2, q)$  is a subgroup of the group of automorphisms of the Paley-Hadamard matrix of order  $q+1$  obtained from the quadratic residues of  $GF(q)$ ,  $q \equiv -1 \pmod{4}$ . If  $q \equiv 1 \pmod{4}$ , there is also an Hadamard matrix of order  $2(q+1)$  obtained from the quadratic residues of  $GF(q)$ . If  $S$  is the matrix of order  $q+1$  obtained from  $\left[ \chi(a_i - a_j) \right]_{a_i \in GF(q)}$ ,  $\chi$  the quadratic character, with a row and column  $\infty$  added,  $\pm 1$ 's in row and column  $\infty$  except 0 at  $(\infty, \infty)$ , then

$$H = H_2 \times I + TH_2 \times S \quad T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

THEOREM. The automorphism group of  $H$  includes  $Z_2 \times PGL_2(q)$ , (the group of  $2 \times 2$  matrices of determinant  $\neq 0$ , modulo the diagonal matrices).

As in [1], the transformations

$$x \rightarrow t^2 x$$

$$x \rightarrow x+a$$

simultaneously on rows and columns leave  $S$  invariant, and also  $I$  since the transformation is the same on rows and columns. The transformation

$$x \rightarrow \frac{1}{x} \chi(x)$$

on both rows and columns also leaves  $S$  invariant  $\left( x \rightarrow \frac{1}{x} \text{ and change sign of row } \chi \text{ if } \chi(x) = -1 \right)$  since

$$\chi(x) \chi(y) \chi\left(\frac{1}{x} - \frac{1}{y}\right) = \chi(y-x) = \chi(x-y)$$

as  $\chi(-1) = 1$ . Since we apply the same transformation to both rows and columns,

this also leaves  $I$  invariant. Finally, the transformation of interchanging rows and columns, and changing the sign of column 1 and row 2 leaves  $H$  and  $TH$  invariant.

The permutation  $x \rightarrow tx$ , with  $t \neq 0$  not a square in  $GF(q)$ , applied to both rows and columns, will leave  $I$  invariant and will change the sign of all elements of  $S$  except those in row and column  $\alpha$ . If now we multiply row and column  $\alpha$  by  $-1$ , we leave  $I$  invariant and change  $S$  into  $-S$ . There is an automorphism of  $H_2$  which takes  $TH_2$  into  $-TH_2$ . This operation together with the one on  $S$  described above, leaves invariant both  $H_2 \times I$  and  $TH_2 \times S$ , and is thus an automorphism of  $H$ . Since the transformations  $x \rightarrow tx$ ,  $x \rightarrow x+a$ ,  $x \rightarrow \frac{1}{x}$  generate the group  $PGL_2(q)$ , the theorem is proved.

#### REFERENCE

1. M. Hall, Jr., "Note on the Mathieu Group  $M_{12}$ ," Archiv der Mathematik, vol. 13, pp. 334-340; 1962.

## PART V

## A PROOF OF THE MACWILLIAMS IDENTITIES

This chapter contains a proof by A. M. Gleason of the relation between the weight-distributions of a code and its orthogonal code, first found by MacWilliams in [1], and an extension of the result.

Let  $V$  be the vector space of dimension  $n$  over a field  $F$ , which for the moment we take as  $GF(p)$ . Let  $\xi$  be a primitive  $p$ -th root of 1. We take  $f$  to be the function on  $V$  with  $f(v) = X^{w(v)} Y^{n-w(v)}$  where  $w$  is the weight function. Then we want to calculate

$$\hat{f}(u) = \sum_{v \in V} X^{w(v)} Y^{u-w(v)} \xi^{\langle u, v \rangle}$$

where  $\langle u, v \rangle$  is the ordinary dot product of  $u$  and  $v$ , a bilinear map of  $V \times V$  into  $F$ , and  $\xi^{\langle u, v \rangle}$  is well-defined since  $\xi^p = 1$ . The sum is easiest if we sum one coordinate at a time: Define  $w(v_i) = 0$  or 1 according as  $v_i = 0$  or  $(v = \langle v_1, v_2, \dots, v_n \rangle)$ . Then

$$\begin{aligned} \hat{f}(u) &= \sum_{v_1, v_2, \dots, v_n} X^{w(v_1) + \dots + w(v_n)} Y^{(1-w(v_1)) + \dots + (1-w(v_n))} \xi^{u_1 v_1 + \dots + u_n v_n} \\ &= \prod_{i=1}^n \left( \sum_{v_i} X^{w(v_i)} Y^{1-w(v_i)} \xi^{u_i v_i} \right) \end{aligned}$$

Now the inner sum is  $Y + (q-1)X$  if  $u_i = 0$  and

$$Y + (\xi + \dots + \xi^{p-1})X = Y - X$$

if  $u_i \neq 0$ . Hence,  $\hat{f}(u) = (Y + (q-1)X)^{n-w(u)} (Y-X)^{w(u)}$ ; Note  $q=p$  for now.

The general Poisson summation formula is then

$$\sum_{v \in A} f(v) = \frac{|A|}{|V|} \sum_{u \in B} \hat{f}(u)$$

where A is any subspace of V and B is its annihilator subspace. This becomes

$$\begin{aligned} \frac{|V|}{|A|} \sum_{v \in A} X^{w(v)} Y^{n-w(v)} &= \frac{|V|}{|A|} \sum_{j=0}^n A_j X^j Y^{n-j} \\ &= \sum_{u \in B} (Y-X)^{w(u)} (Y + (q-1)X)^{n-w(u)} \\ &= \sum_{i=0}^n B_i (Y-X)^i (Y+(q-1)X)^{n-i} \end{aligned}$$

where  $A_i$  and  $B_i$  are the weight-distributions of A and B, respectively.

This simplified calculation suggests the following more ambitious calculation. Let us get the joint distribution of all the different coefficients of the vectors. Let  $f(v) = X_0^{\alpha_0} X_1^{\alpha_1} \dots X_{p-1}^{\alpha_{p-1}}$  where v has

$\alpha_0$  0's,  $\alpha_1$  1's,  $\alpha_2$  2's, ..., . Then

$$\begin{aligned} \hat{f}(u) &= \sum_{v_1, \dots, v_n} X_0^{\alpha_0(v_1) + \dots + \alpha_0(v_n)} \dots X_{p-1}^{\alpha_{p-1}(v_1) + \dots + \alpha_{p-1}(v_n)} \xi^{u_1 v_1 + \dots + u_n v_n} \\ &= \prod_{i=1}^n \left( \sum_{v_i} X_0^{\alpha_0(v_i)} X_1^{\alpha_1(v_i)} \dots X_{p-1}^{\alpha_{p-1}(v_i)} \xi^{u_i v_i} \right) \end{aligned}$$

Here the inner sum is

$$X_0 + X_1 \xi^{u_i} + X_2 \xi^{2u_i} + \dots + X_{p-1} \xi^{(p-1)u_i} = Y(u_i)$$

so

$$\hat{f}(u) = Y(0)^{\alpha_0(u)} Y(1)^{\alpha_1(u)} \dots Y(p-1)^{\alpha_{p-1}(u)}$$

Now if, for example, we take  $F = GF(3)$ , and let  $A_{i,j,k}$  be the number of vectors in  $A$  with  $i$  0's,  $j$  1's,  $k$  2's, then

$$\frac{|V|}{|A|} \sum A_{i,j,k} X^i Y^j Z^k = \sum B_{i,j,k} (X+Y+Z)^i (X+\omega Y+\omega^2 Z)^j (X+\omega^2 Y+\omega Z)^k$$

This formula becomes the MacWilliams formula all over again if we put  $Y = Z$  (which amounts to not distinguishing 1's from 2's; more generally,  $X_1 = X_2 = \dots = X_{p-1}$ ).

To treat the general case, when  $F = GF(q)$  for  $q = p^s$ , just replace  $\langle u, v \rangle$  by  $T(u \cdot v)$ , where  $T$  is the trace from  $GF(p^s)$  to  $GF(p)$  and  $u \cdot v$  is the usual dot product.

#### REFERENCES

1. F. J. MacWilliams, "A Theorem on the Distribution of Weights in a Systematic Code," Bell Sys. Tech. J., vol. 42, pp. 79-94; 1963.

## PART VI

## A SIMPLE CONSTRUCTION OF THE BINARY GOLAY CODE

In this part we give a simple construction of the Golay binary (24,12) code (see [1], [2]) starting from the Hamming code of length 8, without using the quadratic residues mod 23. Thus, we give a straightforward construction of the combinatorial configurations on 23 and 24 objects from the one on 7, the projective plane of order 2.

The binary Hamming code  $H$  can be constructed from the rows of the incidence matrix of the projective plane of order 2, with a coordinate at  $\infty$  defined by an overall parity check, and the vector  $1$  (all coordinates = 1). Thus  $H$  is the set of all vectors gotten from the cyclic shifts of the vector  $(1,1,0,1,0,0,0)$  with a coordinate at  $\infty$  with value 1, the complements of these, and the 0 and 1 vectors.  $H$  is a group; it is equivalent to the code consisting of all vectors  $(z,z)$  and  $(z,z+1)$ , with  $z$  of length 4 and even weight.

Let  $H'$  be the code obtained from  $H$  by reversing the order of the finite coordinates;  $H'$  is equivalent to  $H$  and  $H \cap H' = \{0,1\}$ .

We now form the code of length 24 of all vectors of the form

$$(a+x, b+x, a+b+x) \quad a, b \in H, x \in H'.$$

This code is 12-dimensional, since there is no nontrivial representation of the 0 vector. Since  $H \cap H' = \{0,1\}$  and  $H, H'$  consist of vectors of weight 0,4,8,  $H+H'$  is the set of even weight vectors. If any of  $a, b, a+b, x$  are 0 or 1, it is clear that the above vector has weight  $\geq 8$ . We claim that the minimum weight of the code is in fact 8. Denote the weight of  $w$  by  $|w|$ , and let multiplication of vectors be the usual ( $x^2 = x$  for all  $x$ ). Then

$$|u+v| + 2|uv| = |u| + |v|$$

$$\begin{aligned} & |a+x| + |b+x| + |a+b+x| \\ &= |a+b| + 2|(a+x)(b+x)| + |a+b+x| \\ &= |x| + 2\{|(a+b)(1+x)| + |(a+x)(b+x)|\} \\ &= |x| + 2|a+b + ab + x|. \end{aligned}$$

If  $a, b, a+b, x$  are all of weight 4,  $|ab| = 2$  and  $|a+b+ab| = 6$ , so that  $|a+b+ab+x| \geq 2$ , and the above vector has weight  $\geq 8$ .

The  $(23,11)$  code obtained by deleting one coordinate has minimum weight 7, and thus the spheres of radius 3 about the code vectors are disjoint. The well-known equation

$$2^{12} \left( 1 + 23 + \binom{23}{2} + \binom{23}{3} \right) = 2^{12+11} = 2^{23}$$

shows that these spheres cover the set of vectors of length 23, i.e., the  $(23,11)$  code is close-packed. It therefore follows that given a vector  $v$  of length 24, weight 5, there is a unique vector of weight 8 in the  $(24,12)$  code at distance 3 from  $v$ . It is known that this 5-design, and therefore the  $(24,12)$  code, are unique [3].

We remark that our above definition is equivalent to taking all vectors  $(y, y+a_1, y+a_2)$  with  $y$  of even weight (length 8),  $a_1 \in H$ , and  $y+a_1+a_2 \in H'$ .

#### REFERENCES

1. M.J.E. Golay, "Notes on Digital Coding," Proc. IRE, vol. 37, p.657, 1949.
2. L.J. Paige, "A Note on the Mathieu Groups," Can. J. Math., vol. 9, pp. 15-18, 1957.
3. E. Witt, "Die 5-fach transitiven Gruppen von Mathieu," Abh. Math. Sem. Univ. Hamburg, vol. 12, pp. 256-264, 1938; also "Ueber Steinersche Systeme," ibid., pp. 265-275.



## PART VII

## THE (36,15,6) DESIGNS

In [2] certain difference sets were defined in the two Abelian groups of order 36 which do not have elements of order 9; a very similar set was defined in the group  $S_3 \times S_3$  in [1]. It was shown in [2] that all the Abelian difference sets are equivalent to one of six difference sets. This statement is incorrect: there is a seventh set. The designs defined by these difference sets are studied here.

The difference sets in question are defined as follows: let  $A_3$  be the Abelian group of type (3,3), thought of as the affine plane over  $GF(3)$ . Take four lines of different slopes in  $A_3$ , and associate one line with each element of a group of order 4 ( $Z_4$  or  $K_4 = Z_2 \times Z_2$ ). The difference set is the set of all  $(0, x)$ ,  $0$  the identity in the group of order 4,  $x \in L_0$ , and all  $(i, x)$ ,  $x \in L_i$ . The  $L_i$  have at least a triple intersection, and by translation this may be assumed to be the origin of  $A_3$ . The automorphism group of  $A_3$  may then be used to normalize the set further. The argument in [2] (Theorem 10) is essentially correct, but the conclusion drawn is too strong. In  $K_4 \times A_3$  the argument shows that there are three inequivalent difference sets,  $Q_1'$ ,  $Q_2'$ ,  $Q_3'$ , which correspond to the cases  $L_i$  concurrent (at the origin of  $A_3$ , by normalization),  $0 \notin L_0$  and  $0 \notin L_3$ , respectively. In the case of  $Z_4 \times A_3$  we have the sets  $Q_1$ ,  $Q_2$ ,  $Q_3$  which correspond to  $0 \in L_i$  all  $i$ ,  $0 \notin L_0$ ,  $0 \notin L_3$ , respectively, but [2] neglects the case  $Q_4$ :  $0 \notin L_2$  which is not equivalent to  $Q_3$ , as is the case in  $K_4 \times A_3$ ; there is an automorphism  $\sigma$  such that  $\sigma(1) = 2$  in  $K_4$ , but of course not in  $Z_4$ . It is also clear that the multiplier group of  $Q_4$  consists of exactly two elements, the identity and the automorphism  $x \rightarrow -x$  in  $Z_4$ ,  $\sigma L_2 = L_2$ ,  $\sigma L_0 = L_0$ ,  $\sigma L_1 = L_3$  in  $A_3$ .

We shall now study the  $(v, k, \lambda) = (36, 15, 6)$  designs defined by these difference sets. We shall first show that the automorphisms of the designs, i.e., the permutations  $\tau$  of the group elements which also permute the sets of the form  $D + \alpha$ , are just the obvious automorphisms: each  $\tau$  is of the form  $\beta\tau = \beta\tau + \gamma$ , where  $\sigma, \gamma$  are uniquely determined by  $\tau$ ,  $\sigma$  an automorphism of the group,  $\gamma$  an element of the group.

We shall use  $i, j, m, n$  to denote elements of the group of order 4,  $x, y, z$  elements of  $A_3$ ,  $\alpha, \beta$  elements of the group of order 36,  $\tau$  an automorphism of the design defined by the difference set  $D$  (one of the  $Q_i$  or  $Q_i'$ ), and  $S_0$  the complement of  $L_0$  in  $A_3$ . Let  $L_i^*$  = line through 0 parallel to  $L_i$ .

LEMMA 1. If  $D\tau = D$  then

1.  $(0, L_0)\tau = (0, L_0)$
2.  $(0, L_0+x)\tau = (0, L_0+y)$
3.  $(D+x)\tau = D + y$
4.  $(i, L_i)\tau = (j, L_j)$
5.  $(i, L_i+x)\tau = (j, L_j+y)$
6.  $(0, x)\tau = 0, y$

Proof.  $D \cap (D+(i, x))$  is the set  $(0, S_0 \cap L_{-i}+x)$ ,  $(i, L_i \cap S_0+x)$ , and  $(j, L_j \cap L_{j-i}+x)$   $j \neq 0, i$ , when  $i \neq 0$ ;  $D \cap (D+(0, x)) = (0, S_0 \cap S_0+x) \cup (j, L_j \cap L_j+x)$  for  $j \neq 0$ . Two of the sets  $(j, L_j \cap L_j+x)$  must be empty for  $x \neq 0$  (only the one with  $x \in L_j^*$  is not empty).

It is easy to see from this that  $D \cap (D+\alpha) = D \cap (D+\beta)$ ,  $\alpha \neq \beta$ , if and only if  $\alpha$  and  $\beta$  belong to  $L_0^*$ ,  $\alpha, \beta \neq 0$ . Therefore, if  $L_0^* = (0, x_1, -x_1)$ ,  $D\tau = D$  implies  $\tau$  leaves the sets  $D+x_1$  invariant or interchanges them, and  $(D \cap D+x_1)\tau = D \cap D+x_1 = D \cap D-x_1$ . Thus  $(0, S_0)\tau = (0, S_0)$ . The sets  $D + 0, x$ , and  $x \notin L_0^*$ , are the only sets  $D + \alpha$  such that  $|D \cap D+\alpha_1 \cap D+\alpha| = 3$  ( $|D \cap D+\alpha_1 \cap D+ix| = 2$  for  $i \neq 0$ ). Thus  $\tau$  must permute the sets  $D+0x, x \notin L_0^*$ , which implies 3. The intersection of these six sets is easily seen to be  $(0, L_0)$ , so that  $(0, L_0)\tau = (0, L_0)$ , and this with  $(0, S_0)\tau = (0, S_0)$  implies 6. The triple intersections  $D \cap D+x \cap D+y$ ,  $x, y \notin L_0^*$ ,  $x \neq y$  are either empty or consist of  $(i, L_i)$  if  $x, y \in L_i^*$  ( $x=-y$ ). Thus, since  $\tau$  permutes these sets,  $\tau$  permutes the triple intersections, which proves 4. Part 5 follows from the fact that if  $x, y \notin L_0^*$ ,  $D+x \cap D+y = (0, S_0+x \cap S_0+y) \cup (i, L_i+x)$  with  $y-x \in L_i^*$  (so  $L_i+x = L_i+y$ ). Since the sets  $D+x, x \notin L_0^*$  are permuted by  $\tau$ , and the sets  $(0, L_0+x)$  are also permuted by  $\tau$ , it follows that the sets  $(i, L_i+x)$  also are.

LEMMA 2. If  $\tau$  is any automorphism of the design, and  $(D+i0)\tau = D+jz_1$ , then

1.  $(i, L_0)\tau = (j, L_0+z_1)$
2.  $(i, L_0+x)\tau = (j, L_0+y)$
3.  $(D+ix)\tau = D+jy$
4.  $(i+m, L_m)\tau = (n+j, L_n+z_1)$
5.  $(i+m, L_m+x)\tau = (n+j, L_n+y+z_1)$

Let  $T_\beta$  denote translation by  $\beta$ :  $\alpha T_\beta = \alpha + \beta$  for all  $\alpha$ . Then  $T_1 \tau T_{-jz_1} = \tau'$  leaves  $D$  fixed, and 1-5 follow directly from the corresponding statements of Lemma 1 applied to  $\tau'$ .

The statements of Lemma 2 show that  $\tau$  defines a permutation  $\tau_4$  of the group of order 4, such that  $(D+ix)\tau = D+(i\tau_4)y$ , and  $(ix)\tau = (i\tau_4, z)$  for all  $x \in A_3$ . Note that in 4 and 5  $n = (m+i)\tau_4 - j$ .

LEMMA 3. Let  $\tau$  be any automorphism of the design, and write  $(ix)\tau = i\tau_4$ ,  $x\tau_1$ . Then each  $\tau_1$  is a collineation from the  $i$  plane, the set of  $(i, x)$ , to the plane  $i\tau_4, A_3$ .

This follows from Lemma 2.

LEMMA 4.  $D\tau = D$  implies  $(D+ix)\tau = (D + ((i\tau_4), (x\tau_0)))$ .

Proof. Suppose first  $i \neq 0$ . Since  $D \cap D+ix \cap (0, A_3) = (0, (L_{-i}+x) \cap S_0)$  the sets  $D+ix$  are uniquely defined by their intersection with  $D \cap (0, A_3)$ : this intersection is a pair of points which defines a line, which is parallel to  $L_{-i}$  for some  $i$ . The point  $x$  is then determined uniquely by the fact that these two points are on  $L_{-i}+x$  and not on  $L_0$ . Thus, the formula holds for  $i \neq 0$ , since  $D\tau = D$ , and thus  $(0, A_3)\tau = (0, A_3)$  by Lemma 1. Now, to show the formula holds for  $i=0$ , observe that  $D+x \cap D+iy \cap (0, A_3) = (0, S_0+x \cap L_{-i}+y)$  so that we can recover  $x$  from  $D+x \cap D+iy \cap (0, A_3)$  for all  $i \neq 0$ . Since the formula applies to the sets  $D+iy$ ,  $i \neq 0$ , it therefore applies also to the  $D+x$ .

LEMMA 5.  $ix = \cap D+jy$  for  $j \neq i$ ,  $y-x \in L_{i-j}$ .

It is clear that  $ix$  is in the intersection of the nine sets above (and the six sets  $D+iy$ ,  $x-y \in S_0$ ). If  $nz \in \cap D+jy$  then  $z \in L_{n-j}+y$ , for all  $y$  such that  $y \in L_{i-j}+x$ ,  $j \neq i$ . We then must have  $n=1$ , as otherwise  $z$  belongs to the intersection of three parallel lines. But then  $z=x$ , since  $z-x$  belongs to two different lines through 0, (there are at least two  $L_m = L_{i-j}$  through 0,  $m \neq 0$ ).

LEMMA 6.  $D\tau = D$  implies  $(j-i)\tau_4 = j\tau_4 - i\tau_4$ .

There is, of course, nothing to prove in case the group of order four is  $K_4$ , since then any permutation which preserves 0 is an isomorphism. We need the lemma only to show that  $2\tau_4 = 2$ ,  $2 \in Z_4$ .

Since  $ix = \cap D+jy$ ,  $j \neq i$ ,  $y \in L_{i-j}+x$ , we have  $(ix)\tau = \cap (D+jy)\tau = D+(j\tau_4, y\tau_0)$  by Lemma 4, with  $j \neq i$ ,  $y \in L_{i-j}+x$ . We know that  $(ix)\tau = i\tau_4, z$  for some  $z$ . Examine the elements of the form  $i\tau_4$  in  $\cap (D+jy)\tau$ :  $(i\tau_4, z) \in \cap (D+jy)\tau$  if and only if  $z \in L_{i\tau_4-j\tau_4} + (y\tau_0)$  for all  $j \neq i$ ,  $y \in L_{i-j}+x$ . As before, we see that we must have  $L_{i-j}^* \tau_0 = L_{i\tau_4-j\tau_4}^*$ . But from Lemma 2, part 4, with  $i=-m$ , we see that  $(0, L_m)\tau = (0, L_{-(-m\tau_4)} + z_{-m})$ , so that  $L_i^* \tau_0 = L_{-(-i\tau_4)}^*$ , so we must have  $-(j-i)\tau_4 = i\tau_4 - j\tau_4$ , as asserted. (For  $i=j$  the lemma follows from Lemma 1.)

THEOREM. Any automorphism of one of the designs is just a trivial automorphism ( $x\tau = \alpha x + \beta_0$ , with  $\sigma$  a multiplier).

This theorem destroys the hope that an interesting new permutation group might arise as the automorphism group of one of these designs. It was shown in the last annual report that at most two of the seven designs are isomorphic.

If  $D\tau = D+\alpha$ , we may replace  $\tau$  by  $\tau T_{-\alpha}$ , and so we may assume  $D\tau = D$ . Then from Lemma 6, and Lemma 2, part 4, we have  $(0, L_m)\tau = (0, L_{m\tau_4} + Z_{-m})$  with  $(D+m0)\tau = D+m\tau_4, z_m = D+(m\tau_4, 0\tau_0)$  by Lemma 4;  $D\tau = D$  implies  $0\tau_0 = 0$ , and so  $(0, L_m)\tau = (0, L_{m\tau_4})$ . Thus  $\tau_0$  must take a line  $L_i$  not through 0 into itself,

since  $0\tau_0 = 0$ . But for each of the seven sets, the multiplier group is such that  $L_0$  and any line not through 0 will be preserved, and otherwise the  $L_i$  can be permuted arbitrarily. Thus, by following  $\tau$  by a multiplier as well, we may assume that the lines  $L_i$  are all left invariant, (and in the case  $0 \in L_i$  for all  $i$ , that the plane  $0, A_3$  is left invariant). But then  $\tau_0$  is the identity, and thus by Lemma 4  $\tau$  is the identity.

#### REFERENCES

1. P. Kesava Menon, "On Difference Sets Whose Parameters Satisfy a Certain Relation," Proc. Amer. Math. Soc., vol. 13, pp. 739-745; 1962.
2. R. Turyn, "Character Sums and Difference Sets," Pac. J. Math., vol. 15, pp. 319-346; 1965.

## PART VIII

## THE COVERING RADIUS OF SOME BCH CODES

If we are given an arbitrary block code of block length  $n$  the covering radius is the maximum number of changes that must be made in a word of length  $n$  in order to change it into a code word. Thus, for each word  $w$  of length  $n$  we compute  $\min |w-x|$  for  $x$  in the code, and the maximum of these is the covering radius of the code.

Gorenstein, Peterson, and Zierler have shown that the covering radius of the binary weight  $\geq 5$  BCH codes is 3. We shall derive some facts about the packing radius of some BCH codes with  $q$  odd.

The BCH codes over a field with  $q$  element have length  $q^n-1$ , and are defined as the set of all vectors  $(v_i)$  such that  $\sum v_i \alpha^{ij} = 0$ ,  $j = 1, \dots, t$  with  $\alpha$  a primitive element of  $GF(q^n)$ . Of course for  $j = mq$  the equation  $\sum v_i \alpha^{ij} = 0$  follows from the equation  $\sum v_i \alpha^{im} = 0$ . The maximum weight is  $\geq t + 1$ .

We note that the defining equations for the code could be written

$$\sum_x v_x x^j = 0, \quad x \text{ ranging over the distinct elements of } GF(q^n)^*.$$

To correct a given vector  $v$ , we try to find a vector  $v'$  such that  $v-v'$  is in the code and  $v'$  has weight as small as possible. If  $v = (v_i)$ ,  $v' = (v'_i)$  we let

$$\sum v_i \alpha^{ij} = S_j.$$

Then we must have  $\sum (v_i - v'_i) \alpha^{ij} = 0$ ,  $1 \leq j \leq t$ , so that

$$\sum v'_i \alpha^{ij} = S_j$$

We want  $\sum v'_i x_i^j = S_j$  with  $x_i$  distinct, and as few  $v'_i \neq 0$  as possible. We note that we can drop the requirement of the  $x_i$  being distinct, since we

could always group equal  $x_i$ , and all the corresponding  $v_i$ . We also note that, if  $q = p^s$ ,  $S_j^p = S_{pj}$ , as  $S_j = \sum v_i x_i^j$  implies  $S_j^p = \left( \sum v_i x_i^j \right)^p = \sum v_i x_i^{jp}$ .

For  $t = 1$ , the BCH code has weight 3 if  $q$  is even (we then get the Hamming code), but weight 2 if  $q$  is odd. We can always correct by a weight one vector in exactly  $q-1$  ways: we must solve  $vx = S_1$  with  $v \in GF(q)$ , and for  $S_1 \neq 0$  there are  $q-1$  solutions. For  $t = 2$  and  $q$  odd, we have the following interesting observation.

THEOREM. If  $q$  is odd,  $n > 1$ , the BCH weight  $\geq 3$  code has covering radius 3 if  $n$  is even, 2 if  $n$  is odd,  $q > 3$ . The covering radius is 3 for  $q = 3$ .

Note that for  $q = 3^s$ , the weight is  $\geq 4$ .

We must solve

$$aX + bY = S_1$$

$$aX^2 + bY^2 = S_2$$

with  $S_i$  arbitrary elements of  $GF(q^n)$  if the covering radius is to be 2. If  $S_1 \neq 0$ , take  $a = 1$ ,  $b = -1$ :

$$X - Y = S_1$$

$$X^2 - Y^2 = S_2 \quad \text{or} \quad X + Y = \frac{S_2}{S_1}$$

which can always be solved. Thus we can correct all the vectors, except those lying in the BCH code for  $t = 1$ , by a weight 2 vector. (We can correct by a

weight 1 vector if  $S_1 S_2 \neq 0$  and  $\frac{S_1^2}{S_2} \in GF(q)$ .)

If  $S_1 = 0$ , we would have

$$aX + bY = 0$$

$$aX^2 + bY^2 = S_2$$

or

$$\left(a + \frac{a^2}{b}\right)X^2 = S_2$$

$$X^2 = \frac{b S_2}{a(a+b)} = \frac{S_2}{c(c+1)} \quad c = \frac{a}{b}$$

This equation can be solved in  $GF(q^n)$  if and only if  $\frac{S_2}{c(c+1)}$  is a square, and of course  $S_2$  need not be a square. In that case we try to make  $c(c+1)$  also not a square. This is possible only when  $n$  is odd, since when  $n$  is even,  $GF(q^n) \supset GF(q^2)$ , and  $GF(q^2)$ , being the unique field of degree 2 over  $GF(q)$ , is obtained by adjoining the square root of any nonsquare in  $GF(q)$ .

However, for  $q = 3$ ,  $S_2$  a square in  $GF(q^n)$ ,  $c(c+1) = 0$  or  $-1$  for  $c \in GF(q)$ ;  $c(c+1) = 0$  is impossible. For  $q = 3$  and  $S_1 = 0$ ,  $S_2$  a square, we cannot solve the equations in two unknowns. We can always solve in three unknowns by the simple device of reducing to the case  $S_1 \neq 0$  by a weight 1 vector, and then correcting by a weight 2.



## PART IX

## ON THE PETERSON, ET AL. AFFINE-INVARIANCE THEOREM

Peterson [1] has proved that extended BCH codes are invariant under the affine group, and Kasami, Lin, and Peterson [2] found necessary and sufficient conditions for an extended cyclic code to be affine-invariant. This report gives two slight extensions of the latter result; namely, it shows that the extension of the code is unique and that fewer computations are needed to verify whether a given code is affine-invariant.

A cyclic code of length  $q^k-1$  over  $F = GF(q)$  can be regarded as the set  $C$  of all functions  $h$  with values in  $F$  defined on the multiplicative group  $K^\times$  of  $K = GF(q^k)$  satisfying

$$\sum_{\alpha \in K^\times} h(\alpha) \alpha^i = 0 \quad i \in I \quad (1)$$

for an index set  $I$  defined by the condition that  $\zeta^i$  is a root of the generator polynomial  $g(x)$  of the code for a fixed primitive element  $\zeta$  of  $K$ . In particular, we choose  $I$  to be contained in  $0, 1, \dots, q^k-2$ . This statement is easily verified if one thinks of  $h(\alpha)$  as the  $j$ -th coordinate of a code-vector, where  $\alpha = \zeta^j$ .

That the code is cyclic is the same as saying that  $h \in C$  implies  $h_\beta \in C$  for every  $\beta \in K^\times$ , where  $h_\beta(\alpha)$  is defined as  $h(\beta\alpha)$  for each  $\alpha \in K^\times$ .

We shall derive a set of necessary and sufficient conditions on the code and on the definition of  $h$  at 0, i.e., on how to extend the code, so that the extended code is invariant under the affine group  $(x \mapsto ax+b)$  of  $K$ . That is, we get a new "code"  $C'$  by extending each function  $h$  to  $K$  by assigning, in any way at all, a value  $h(0)$ , and we ask under what conditions on  $h(0)$  and the code  $C$  we get affine invariance for  $C'$ .

We need only check for translation. Let  $\beta \in K^\times$ . Then  $C'$  is affine-invariant if and only if

$$\left. \begin{array}{l} \sum_{\alpha \in K^X} h(\alpha + \beta) \alpha^i = 0 \quad i \in I, \beta \in K^X \\ \text{and} \\ h(\beta) = h^\beta(0) \end{array} \right\} \quad (2)$$

where  $h^\beta(\alpha) = h(\alpha + \beta)$ ,  $\alpha \in K$ . condition (2) implies  $h^\beta \in C$ .

Note that 0 cannot be in I if condition (2) holds unless the code is the 0-code, for then we would have

$$h(0) = - \sum_{\alpha \neq 0, \beta} h(\alpha)$$

for all  $\beta \in K^X$ . This means  $h(\beta) = h(\beta')$  for all  $\beta, \beta' \in K^X$ , and thus  $h(\alpha) = c$  for all  $\alpha \in K$ . Now condition (1) implies  $c = 0$ .

Now condition (2) holds if and only if

$$\left. \begin{array}{l} \sum_{\alpha \in K} h(\alpha) (\alpha - \beta)^i = 0, \quad i \in I, \beta \in K^X \\ \text{and} \\ h(\beta) = h^\beta(0) \end{array} \right\} \quad (3)$$

Note that the sum in condition (3) is now purposely over all  $\alpha$  in  $K$  and that the unwanted term  $h(\beta)$  does not enter. condition (3) is equivalent to

$$\left. \begin{array}{l} \sum_{j=0}^i \binom{i}{j} (-1)^j \left( \sum_{\alpha \in K} h(\alpha) \alpha^j \right) \beta^{-j} = 0 \quad i \in I, \beta \in K^X \\ \text{and} \\ h(\beta) = h^\beta(0). \end{array} \right\} \quad (4)$$

If we set  $\gamma_j = (-1)^j \sum_{\alpha \in K} h(\alpha) \alpha^j$ , then condition (4) is equivalent to saying that the polynomial

$$\sum_{j=0}^i \binom{i}{j} \gamma_j x^j$$

has each  $\beta^{-1}$  in  $K$  as a root [and  $h(\beta) = h^\beta(0)$ ]. This means that, since  $i < q^k - 1$ ,

$$\text{for } j=0, 1, \dots, i, \binom{i}{j} \gamma_j = 0, i \in I, \text{ and } h(\beta) = h^\beta(0) \quad (5)$$

and conversely.

The meaning of the binomial theorem is in particular that  $\gamma_0 = \sum_{\alpha \in K} h(\alpha)$ . Since  $\binom{i}{0} = 1$  for all  $i \in I$ , we find that condition (5) is equivalent to

$$\sum_{\alpha \in K} h(\alpha) = 0 \quad \text{for all } h \in C',$$

and for each  $i \in I$ , every  $j$  in the range  $0 < j < i$  satisfies either  $j \in I$  or  $\binom{i}{j} \equiv 0 \pmod{p}$

(6)

where  $q = p^s$  for the prime  $p$ .

To see that condition (5) implies condition (6) notice that  $\gamma_0 = 0$  is not the condition that  $0 \in I$ , but that  $\gamma_j = 0$  for  $0 < j < i$  is the condition that  $j \in I$ . For the converse, we need only to show that  $h(\beta) = h^\beta(0)$  for each  $\beta \in K$ . Now

$$h^\beta(0) = - \sum_{\alpha \neq 0} h^\beta(\alpha) = - \sum_{\alpha \neq 0} h(\alpha + \beta) = h(\beta) - \sum_{\alpha \in K} h(\alpha + \beta) = h(\beta)$$

We have proved the Kasami-Lin-Peterson theorem and have shown that this definition of  $h(0)$  is the only definition that admits the affine group as automorphisms.

One can write  $\begin{pmatrix} i \\ j \end{pmatrix} \equiv \prod \begin{pmatrix} i_m \\ j_m \end{pmatrix} \pmod{p}$ , where  $i = \sum i_m p^m$  and  $j = \sum j_m p^m$  with

$0 \leq i_m, j_m < p$ ; then Condition (6) becomes

$$\left. \begin{aligned} \sum_{\alpha \in K} h(\alpha) &= 0 \\ \text{and for each } i \in I, \text{ and } j \text{ satisfying } 0 < j < i, j_m \leq i_m \text{ for all } m \\ \text{implies } j \in I. \end{aligned} \right\} (7)$$

It is possible to weaken the hypothesis of Condition (7) as follows. Let  $\zeta$  be a primitive root of 1 of order  $q^k - 1$ , and let the roots of the generator polynomial  $g(x)$  be  $\zeta^i$ , where  $i$  runs over a set  $I$  contained in  $\{0, 1, \dots, q^k - 2\}$ . Since  $g(x)$  has coefficients in  $GF(q)$ ,  $I$  consists of a union of orbits under multiplication by  $q$  (and reduction mod  $q^k - 1$ ):  $I = C_1 \cup \dots \cup C_t$ .

LEMMA. From each orbit select one integer  $i'$ . Suppose that for each such  $i'$  we have:  $0 < j < i'$  implies  $\begin{pmatrix} i' \\ j \end{pmatrix} \equiv 0 \pmod{p}$  or  $j \in I$ . Then the same is true for each  $i \in I$ ; in other words, the cyclic code generated by  $g(x)$ , when extended as above, is invariant under the affine group if and only if Condition (7) holds for one value of  $i$  from each orbit.

Proof. We use, of course, the well-known relation mentioned above:

$$\begin{pmatrix} i \\ j \end{pmatrix} \equiv \begin{pmatrix} i_0 \\ j_0 \end{pmatrix} \cdot \dots \cdot \begin{pmatrix} i_N \\ j_N \end{pmatrix} \pmod{p}$$

where  $i = \sum_0^N i_n p^n$  and  $j = \sum_0^N j_n p^n$ , with  $0 \leq i_n, j_n < p$ . ( $p^{N+1} = q^h$ .) Notice that we must reduce each integer under consideration mod  $q^k - 1$  to a value between 0 and  $q^k - 2$ . Since  $q^k \equiv 1 \pmod{q^k - 1}$  we find that  $qi$  has, in our terms, coefficients of its base- $p$  expansion which are a cyclic shift of those of  $i$ .

Now suppose  $i$  is any element of  $I$  and let  $i'$  be the element in the orbit of  $i$  satisfying the hypothesis of the Lemma. Let  $0 < j < i$  and suppose  $\begin{pmatrix} i \\ j \end{pmatrix} \not\equiv 0 \pmod{p}$ . This means  $i_n \geq j_n$  for every  $n$ . Multiply  $i$  by  $q^m$  to move  $i$  to  $i'$ . Let  $j'$  be the element in the orbit of  $j$  congruent to  $q^m j$ . Then, since

both the  $i_n$ 's and the  $j_n$ 's have been cyclically shifted by the same amount, we have  $0 < j' < i'$  and  $\binom{i'}{j'} \not\equiv 0 \pmod{p}$ . Therefore  $j' \in I$ , hence  $j \in I$ .

#### REFERENCES

1. W. W. Peterson, "On the Weight Structure and symmetry of BCH Codes," Scientific Report AFCRL-65-515, Air Force Cambridge Research Labs., Bedford, Mass., July 10, 1965.
2. T. Kasami, S. Lin, W. Peterson, "Some Results on Cyclic Codes which are Invariant Under the Affine Group," Scientific Report AFCRL-66-622, Air Force Cambridge Research Labs., Bedford, Mass., August 15, 1966.

**BLANK PAGE**

## PART X

## FACTORIZATION OF CYCLOTOMIC POLYNOMIALS OVER CERTAIN QUADRATIC NUMBER FIELDS

We calculated some factorizations which we record here.

If  $\ell$  is a rational odd prime the polynomial  $X^\ell - 1$  has a root field of degree  $\ell-1$  over the rational field  $Q$ . This field has a unique quadratic subfield  $L = Q(\sqrt{\pm\ell})$ , where the sign is such that  $\pm\ell \equiv +1 \pmod{4}$ . Let  $z$  be a primitive  $\ell$ -th root of 1 over  $Q$ . The subfield  $L$  is also generated by  $\eta$ , where  $\eta = \sum z^r$ , the sum over  $r$  in  $R$ , the set of all quadratic residues modulo  $\ell$ .  $\eta$  and its conjugate  $\bar{\eta}$  are the roots of  $x^2 + x + (1 \pm \ell)/4$ ; here the opposite sign is chosen, so that the constant term is an integer. In particular, they satisfy  $\eta + \bar{\eta} = -1$ . The polynomials we wish to calculate are

$$g(X) = \prod_{r \in R} (X - z^r) \quad \text{and} \quad \bar{g}(X) = \prod_{r \in R} (X - z^{sr})$$

where  $s$  is a fixed quadratic nonresidue mod  $\ell$ . Thus  $\bar{g}(X)$  is the conjugate of  $g(X)$ .

To start with we observe that if  $\ell \equiv -1 \pmod{4}$ , then  $-1 \notin R$  and, therefore,

$$\bar{g}(X) = -X^{(\ell-1)/2} g(X^{-1})$$

since the constant terms are  $(-1)^{(\ell-1)/2} N(z) = -Nz$  and  $-Nz^s$ ,  $N$  being the norm from  $Q(z)$  to  $L$ . Since  $1 = Nz \cdot Nz^s = (Nz)^{1+s} = (Nz)^\ell$  for every quadratic nonresidue  $s \pmod{\ell}$ ,  $Nz$  must be 1 if  $\ell > 3$ . In other words, the sum of all  $r$  in  $R$  is divisible by  $\ell$  if  $\ell > 3$ . (This is true for any prime  $\ell > 3$ .) And alternatively, the sum of all the elements in any multiplicative subgroup of  $GF(\ell)^\times$  is 0, as the sum of all the roots of 1 of a given order in a field.

Next we have, setting  $m = (\ell-1)/2$ ,

$$g(X) = X^m - \eta X^{m-1} + \dots + \bar{\eta} X - 1$$

$$\bar{g}(X) = X^m - \bar{\eta} X^{m-1} + \dots + \eta X - 1$$

for the case  $\ell \equiv -1 \pmod{4}$ . This already settles the case  $\ell=7$ :

$$\left. \begin{aligned} g(X) &= X^3 - \eta X^2 + \bar{\eta} X - 1 \\ \bar{g}(X) &= X^3 - \bar{\eta} X^2 + \eta X - 1 \\ (x-\eta)(x-\bar{\eta}) &= x^2 + x + 2 \end{aligned} \right\} \ell = 7.$$

For higher values of  $\ell$ , we need to use such things as

$$R \div R = \frac{(\ell+1)}{4} R' + \frac{\ell-3}{4} R(\ell=4v-1)$$

the meaning of which is explained in our 1966 report, pages III-33 ff. We find

$$\left. \begin{aligned} g(X) &= X^5 - \eta X^4 - X^3 + X^2 - (1+\eta)X - 1 \\ (x-\eta)(x-\bar{\eta}) &= x^2 + x + 3 \end{aligned} \right\} (\ell = 11)$$

$$\left. \begin{aligned} g(X) &= X^6 - \eta X^5 + 2X^4 - (1+\eta)X^3 + 2X^2 - \eta X + 1 \\ (x-\eta)(x-\bar{\eta}) &= x^2 + x - 3 \end{aligned} \right\} (\ell = 13)$$

$$\left. \begin{aligned} g(X) &= X^{11} - \eta X^{10} - (3+\eta)X^9 - 4X^8 + (\eta-3)X^7 \\ &\quad + (2\eta-1)X^6 - (2\bar{\eta}-1)X^5 - (\bar{\eta}-3)X^4 + 4X^3 \\ &\quad + (3+\bar{\eta})X^2 + \bar{\eta} X - 1 \\ (x-\eta)(x-\bar{\eta}) &= x^2 + x + 6 \end{aligned} \right\} (\ell = 23)$$



## PART XI

## A THEOREM OF GLEASON AND PIERCE\*

The following is a slightly shorter proof of a theorem proved by J. Pierce and A. Gleason. Only the second part of the proof is different. The question is the existence of codes which are formally self-orthogonal, i.e., have the same weight distribution as their orthogonal complements and in which the vectors all have weight a multiple of the integer  $t$ . Examples of such codes are the extended quadratic residue codes over  $GF(2)$  in which all vectors have weight a multiple of 4, the extended cyclic  $(13, 6)$  code over  $GF(4)$  in which all vectors have even weight, the set of even weight vectors in any group code over  $GF(2)$ , and the extended quadratic residue codes for primes of the form  $12k-1$  over  $GF(3)$  with  $t = 3$ .

Let  $A_i, B_i$  denote the number of vectors of weight  $i$  in a group code over  $GF(q)$  and its orthogonal complement, respectively, and

$$\alpha(x,y) = \sum A_i x^i y^{n-i}, \quad \beta(x,y) = \sum B_i x^i y^{n-i}$$

with  $n$  = code length,  $k$  = dimension of the group code. The MacWilliams identity states that

$$\alpha(y-x, y+(q-1)x) = q^k \beta(x,y)$$

or, in nonhomogeneous form, with  $x/y = z$ ,

$$(1 + (q-1)x)^n \alpha\left(\frac{1-z}{1+(q-1)z}, 1\right) = \beta(z, 1)$$

---

\* This is a corrected version of Section VIII of our Report of April 28, 1965, under Contract No. AF19(604)-8516.

Thus, if the group code is formally self-orthogonal, we have  
 $\alpha(x,y) = \beta(x,y)$  and

$$\alpha(y-x, y + (q-1)x) = q^{n/2} \alpha(x,y)$$

If  $A_i = 0$  unless  $i = kt$ , i.e., all the weights are multiples of  $t$ , then  
 $\alpha(x,y) = \alpha(\omega x, y)$  if  $\omega^t = 1$ .

Let  $T_1, T_2$  be the fractional linear transformations

$$T_1(z) = \frac{1-z}{1+(q-1)z}$$

$$T_2(z) = \omega z$$

If  $\alpha$  is the polynomial associated with a formally self-orthogonal code with all vectors of weight a multiple of  $t$ , then  $T_1, T_2$  operate on the "homogeneous" roots of  $\alpha$  (we allow  $\lambda = \infty$  with the usual conventions:  $\alpha, \beta$  are homogeneous polynomials and  $(a, b)$  is a root of  $\alpha$  if  $bx - ay$  divides  $\alpha$ . Since  $\alpha$  is a homogeneous polynomial,  $(a, b)$  is a root if and only if  $(sa, sb)$  is a root for nonzero  $s$ , and thus the roots of  $\alpha$  should be thought of as points of the Riemann sphere);  $\alpha(\lambda, 1) = 0$  implies  $\alpha(T(\lambda), 1) = 0$  if  $T = T_1$  or  $T_2$  and this holds for any  $T$  in the group  $G$  generated by  $T_1$  and  $T_2$ . Thus the set of roots of  $\alpha$  on the Riemann sphere is closed under  $G$ .

But if  $G$  is any group of fractional linear transformations and a finite orbit contains three distinct points,  $G$  is finite. For the number of distinct triples of points from the orbit is finite, and since a fractional linear transformation leaving three points fixed is the identity,  $G$  is finite.

We conclude that the group  $G$  generated by  $T_1$  and  $T_2$  is finite for  $t \neq 2$ . For then if  $\lambda$  is any root of  $\alpha$  not 0 or  $\infty$ ,  $\lambda \omega^i$  are  $t$  distinct roots of  $\alpha$  if  $\omega$  is a primitive  $t$ -th root of 1. (If  $\lambda = 0$  or  $\infty$ ,  $T_1(\lambda) = \frac{1}{1-q}$  or 1, another root of  $\alpha$ .) If  $t = 2$ ,  $T_1(z) = z$  only for  $z = \frac{-1 \pm \sqrt{q}}{q-1}$  and  $T_1(z) = -z$  for  $z = \pm \frac{1}{\sqrt{1-q}}$ .

The set of roots of  $\alpha(x,y)$  can consist of two values only for  $\lambda = \pm \frac{1}{\sqrt{1-q}}$ , as otherwise  $\lambda, -\lambda, T_1(-\lambda)$  will be distinct. Therefore, we must have  $\alpha(x,y) = c(y^2 + (q-1)x^2)^{n/2}$  with  $c$  constant (and thus clearly 1). In fact, the direct product of the code  $\{(\alpha, \gamma\alpha)\}$ ,  $\gamma^2 + 1 = 0$ , with itself  $n/2$  times has this distribution and is self-orthogonal. Except in this case, every element of  $G$  must be of finite order since  $G$  is finite.  $T_1 T_2 = \frac{1-\omega z}{1+(q-1)\omega z}$  must be of finite order, i.e., some power of the matrix

$$\begin{pmatrix} -\omega & 1 \\ (q-1)\omega & 1 \end{pmatrix}$$

must be a scalar multiple of the identity matrix (the identity as a projective transformation). We assume that  $\omega \neq 1$ .

The eigenvalues  $x_1, x_2$  of  $T_1 T_2$  satisfy the equation

$$x^2 + (\omega-1)x - \omega q = 0$$

If  $(T_1 T_2)^m = cI$ , we must have  $\left(\frac{x_1}{x_2}\right)^m = 1$ , i.e.,  $\frac{x_1}{x_2}$  is a root of 1. Then

$$2 + \frac{x_1}{x_2} + \frac{x_2}{x_1} = 2 + \frac{x_1^2 + x_2^2}{x_1 x_2} = \frac{(x_1 + x_2)^2}{x_1 x_2} = \frac{-(\omega-1)^2}{\omega q}$$

is an algebraic integer, and  $q$  divides  $(\omega-1)^2$ . But if  $\omega$  is a  $t$ -th root of 1,  $1-\omega$  is a unit if  $t$  is not a prime power and  $(1-\omega)^{\phi(t)} = (p)$  if  $t = p^j$  (an equation of ideals). Thus we must have  $\phi(t) = 1$  or 2. If  $\phi(t) = 1$ ,  $t = 2$  and  $\omega = -1$ . Then  $\frac{4}{q}$  is an algebraic integer, and  $q = 2$  or 4.

If  $\phi(t) = 2$ ,  $t = 3, 4$ , and  $6$ . However,  $t = 6$  is impossible, since if  $\omega$  is a primitive 6-th root of 1 we should have  $-\frac{(\omega-1)^2}{\omega q} = \frac{1}{q}$  an algebraic integer, which is impossible. If  $t = 3$  and  $\omega$  is a cube root of 1,  $-\frac{(\omega-1)^2}{\omega} = 3$ , and thus we must have  $q = 3$ . Finally, if  $t = 4$ , we can let  $\omega = i$ :  $\frac{2}{q}$  must be an integer, and  $q = 2$ .

We thus have the possibilities

| t | q    |
|---|------|
| 2 | 2, 4 |
| 3 | 3    |
| 4 | 2    |